

UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

LURIAN VIEIRA SERAFIM

**ANÁLISE DE SEGURANÇA EM REDES *WIRELESS* POR MEIO DO TESTE DE
PENETRAÇÃO**

CRICIÚMA
2020

LURIAN VIEIRA SERAFIM

**ANÁLISE DE SEGURANÇA EM REDES WIRELESS POR MEIO DO TESTE DE
PENETRAÇÃO**

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. Me. Paulo João Martins

CRICIÚMA

2020

LURIAN VIEIRA SERAFIM

**ANÁLISE DE SEGURANÇA EM REDES *WIRELESS* POR MEIO
DO TESTE DE PENETRAÇÃO**

Trabalho de Conclusão de Curso
aprovado pela Banca
Examinadora para obtenção do
Grau de Bacharel, no Curso de
Ciência da Computação da
Universidade do Extremo Sul
Catarinense, UNESC, com Linha
de Pesquisa em Segurança da
Informação

Criciúma, 06 de agosto de 2020.

BANCA EXAMINADORA

DocuSigned by:
PAULO JOÃO MARTINS
2C63A5088FBE4A5...

Prof. Me. Paulo João Martins - (UNESC) – Orientador

DocuSigned by:
Rogério Antônio Casagrande
91F9FA28636E4C3...

Prof. Dr. Rogério Antônio Casagrande - (UNESC)

Prof. Me. Valter Blauth Junior - (UNESC)

DocuSigned by:
Valter Blauth Junior
87352B030E8943B...

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ter me dado essa grande oportunidade e ter me permitido alcançar essa vitória em minha vida.

Agradeço a minha família em especial minha mãe Edina Rosalba Vieira, minha irmã Patrícia Vieira Coral e meu cunhado Leandro Cardozo que me deram todo o suporte nos momentos difíceis e nunca me deixaram desistir dos meus sonhos. A minha prima Samara Cardoso Teixeira por ter me auxiliado no início de tudo, para que eu ganha-se a bolsa de estudos que me possibilitou chegar a esse momento.

A minha prima Jheniffer Vieira Paulino, por nunca me deixar desanimar e sempre ter uma palavra de ânimo nos momentos difíceis da vida. As minhas amigas Ineida Teixeira Pereira, Cleide Zilii Donadel e Ide Frasson por sempre torcer por min, dizendo que eu era capaz perante os desafios que apareciam no caminho. Aos meus amigos Ana Olga Teixeira, Fernando Felipe e Eldori Antônio dos Santos por ter me auxiliado com o transporte. Aos Meus tios Rosane Maria Vieira, Loraci Mateus e Joésio Vieira que gentilmente abriram as portas de suas casas para que eu passasse a noite, e pode-se ir as aulas dos finais de semana.

Ao meu padrinho Ricardo Teixeira Canarina por sempre me dar toda ajuda necessária e sempre estar presente em minha vida. Aos Meus colegas de classe em especial ao meu amigo Clayton Mariano de Andrade por sempre dividir as matérias, trabalhos e auxílios em geral estando sempre pronto a ajudar.

Aos programas do governo Enem e Prouni por me conceder a bolsa de estudos que foi fundamental nessa conquista, pois se não fosse assim não teria condições financeiras de arcar com os custos. A Unesc juntamente com os meus professores, por sempre estarem empenhados em oferecer um ensino de qualidade.

E um agradecimento em especial a minha amiga Gisele Feliciano Joaquim por ter me fornecido todo o suporte necessário para realização do presente trabalho, algo que foi de fundamental importância e que vou lembrar sempre com muito carinho.

RESUMO

As redes Wireless se tornaram de extrema importância na vida da sociedade atual, sendo utilizada todos os dias, tanto no meio residencial quanto no empresarial, atraídos pela fácil instalação e utilização para os mais diversos afazeres quando o assunto é Internet. Por conta dessa popularidade cada vez mais redes *Wireless* vem sendo invadidas para a obtenção de dados de maneira ilícita. Além disso, cada vez mais são descobertos novos problemas na segurança dos AP's, que possibilitam ainda novos métodos de ataques. Pensando nesse problema em 2018 foi anunciada o novo protocolo WPA3, com intuito de ter um protocolo mais robusto e fornecer maior segurança. Porém, já no ano de 2019, vulnerabilidades foram encontradas neste protocolo, a maioria delas herdadas de seu antecessor o WPA2. O presente trabalho tem por objetivo realizar teste de segurança por meio de *Pentest*, com a finalidade de análise dos protocolos WEP, WPA e WPA2, e revisão bibliográfica da segurança do protocolo WPA3, onde as informações foram obtidas por meio de artigos científicos. Sendo apontado os métodos utilizados visando aumentar a segurança nas redes *Wireless*.

Palavras-chave: Segurança da Informação. Redes Wireless. WPA3. WPA2. Pentest.

ABSTRACT

Wireless networks have become extremely important in the life of today's society, being used every day, both in the residential and business environment, attracted by the easy installation and use for the most diverse tasks when it comes to the Internet. Because of this popularity more and more wireless networks are being invaded to obtain data in an illicit way. In addition, more and more new problems are discovered in the security of the AP's, which still make possible new methods of attacks. Thinking about this problem in 2018, the new WPA3 protocol was announced, in order to have a more robust protocol and provide greater security. However, already in 2019, vulnerabilities were found in this protocol, most of them inherited from its predecessor WPA2. The objective of the present study is to perform a Pentest security test to analyze the WEP, WPA, and WPA2 protocols, and to review the WPA3 protocol security literature, where the information was obtained through scientific articles. The methods used were pointed out aiming at increasing security in wireless networks.

Keywords: Information Security. Wireless Networks. WPA3. WPA2. Pentest.

LISTA DE ILUSTRAÇÕES

FIGURA 1 - DISPOSITIVOS CONECTADOS À REDE WIRELESS	17
FIGURA 2 - MODULAÇÃO DE SINAL FHSS	19
FIGURA 3 - MODULAÇÃO DE SINAL DSSS	19
FIGURA 4 - MODULAÇÃO DE SINAL OFDM	20
FIGURA 5 - ESTRUTURA DE CAMADAS DO PADRÃO IEEE 802.11	26
FIGURA 6 - REPRESENTAÇÃO GRÁFICA DO ATAQUE DE AUTENTICAÇÃO.	28
FIGURA 7 - A MÁQUINA DO ATACANTE ESTÁ ATUANDO COMO UM ROGUE ACCESS POINT	31
FIGURA 8 - MITM-FLUXO DO FRAMEWORK	32
FIGURA 9 - ATAQUE KRACK	34
FIGURA 10 - PROCESSO DE AUTENTICAÇÃO EM REDES WPA ENTERPRISE.....	35
FIGURA 11 - WEP, WPA, WPA2, WPA3.....	36
FIGURA 12 - ESTATÍSTICAS DOS INCIDENTES REPORTADOS AO CERT.BR.....	48
FIGURA 13 - PADRÕES/FASES PARA APLICAÇÃO DO <i>PENTEST</i>	50
FIGURA 14 - CENÁRIOS DOS TESTES	62
FIGURA 15 - PREPARAÇÃO DO SISTEMA OPERACIONAL.....	64
FIGURA 16 - CONFERINDO MODO MONITOR	65
FIGURA 17 - VARREDURA DE REDE E CAPTURA DAS INFORMAÇÕES DOS PACOTES	66
FIGURA 18 - AP FALSO.....	67
FIGURA 19 - ATAQUE DE DESAUTENTIFICAÇÃO	67
FIGURA 20 - ATAQUE EVIL TWIN.....	68
FIGURA 21 - ATAQUE DE WPS.....	70
FIGURA 22 - ATAQUE DE WPS.....	70
FIGURA 23 - DEFINIÇÃO DO PROTOCOLO WEP VERSÃO 64BITS E SENHA NO AP	71
FIGURA 24 - DEFINIÇÃO DO PROTOCOLO WEP VERSÃO 128BITS E SENHA NO AP.....	72
FIGURA 25 - CAPTURANDO OS PACOTES ARP	73
FIGURA 26 - QUEBRA DO PROTOCOLO WEP-64BITS E CAPTURA DA SENHA.....	74
FIGURA 27 - QUEBRA DO PROTOCOLO WEP-128BITS E CAPTURA DA SENHA.....	74
FIGURA 28 - DEFINIÇÃO DO PROTOCOLO WPA-AES E SENHA NO AP	75
FIGURA 29 - DEFINIÇÃO DO PROTOCOLO WPA-TKIP E SENHA NO AP	76
FIGURA 30 - QUEBRA DO PROTOCOLO WPA-AES E CAPTURA DA SENHA.....	77
FIGURA 31 - QUEBRA DO PROTOCOLO WPA-TKIP E CAPTURA DA SENHA	77
FIGURA 32 - DEFINIÇÃO DO PROTOCOLO WPA2-AES E SENHA NO AP	78

FIGURA 33 - DEFINIÇÃO DO PROTOCOLO WPA2-TKIP E SENHA NO AP	78
FIGURA 34 - QUEBRA DO PROTOCOLO WPA2-AES E CAPTURA DA SENHA.....	79
FIGURA 35 - QUEBRA DO PROTOCOLO WPA2-TKIP E CAPTURA DA SENHA.....	80
FIGURA 36 - DIAGRAMA HANDSHAKE DE QUATRO VIAS E ENVIO DE PACOTES	82
FIGURA 37 - DIAGRAMA DO HANDSHAKE DE LIBÉLULAS	83

LISTA DE QUADROS

QUADRO 1 - AP'S UTILIZADOS	59
QUADRO 2 - ESPECIFICAÇÕES DOS EQUIPAMENTOS	59
QUADRO 3 - PROGRAMAS UTILIZADOS	61

LISTA DE TABELAS

TABELA 1 - ESTATÍSTICAS DE CYBERCRIMES	15
TABELA 2 - PRINCIPAIS EMENDAS DO IEEE 802.11	22

LISTA DE ABREVIATURAS E SIGLAS

ADSL	<i>Asymmetric Digital Subscribe Line</i>
AES	<i>Advanced Encryption Standard</i>
AP	<i>Access Point</i>
CBC	<i>Cipher-Block Chaining</i>
CCMP	<i>Cipher Block Chaining Message Authentication Code Protocol</i>
CDMA	<i>Code Division Multiple Access</i>
CSMA/CA	<i>Carrier Sense Multiple Access with Collision Avoidance</i>
CTR	<i>Counter Mode</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
EAP	<i>Extensible Authentication Protocol</i>
EAPOL	<i>Extensible Authentication Protocol</i>
ECC	<i>Elliptic Curve Cryptography</i>
FHSS	<i>Frequency Hopping Spread Spectrum</i>
GTK	<i>Group Temporal Key</i>
HMAC	<i>Hash Message Authentication Protocol</i>
HR-DSSS	<i>High Rate Direct Sequence Spread Spectrum</i>
IAPP	<i>Inter-Access Point Protocol</i>
ICV	<i>Integrity Check Value</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
ISO	<i>Open System Interconnection</i>
IV	<i>Initialization Vector</i>
MAC	<i>Media Access Control</i>
MIC	<i>Message Integrity Code</i>
MITM	<i>Man-in-the-Middle</i>
MU-MIMO	<i>Multi-User MIMO</i>
OFDM	<i>Orthogonal Frequency Division Multiplexing</i>
ONU	<i>Organização das Nações Unidas</i>
OWE	<i>Opportunistic Wireless Encryption</i>
PBKDF2	<i>Password-Based Key Derivation Function 2</i>
PHY	<i>Physical Layer</i>
PMF	<i>Protected Management Frameworks</i>

PMK	<i>Pairwise Master Key</i>
PMKID	<i>Pairwise Master Key Identification</i>
PSK	<i>Pre-Shared Key</i>
PTK	<i>Pairwise Transient Key</i>
QAM	<i>Quadrature Amplitude Modulation</i>
QoS	<i>Quality of Service</i>
RC4	<i>Rivest Cipher 4</i>
RM-OSI	<i>Reference Model Open System Interconnection of the International Standardization Organization</i>
RSN	<i>Robust Security Network</i>
SA	<i>Security Association</i>
SAE	<i>Simultaneous Authentication of Equals</i>
SSID	<i>Service Set Identifier</i>
TK	<i>Temporal Key</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
TSC	<i>TKIP Sequence Counter</i>
WEP	<i>Wi-Fi Protected Access</i>
WLAN	<i>Wireless Local Area Network</i>
WPA	<i>Wi-Fi Protected Acces</i>
WPA2	<i>Wi-Fi Protected Acces II</i>
WPA3	<i>Wi-Fi Protected Acces III</i>
WWiSE	<i>Word Wide Spectrum Efficiency</i>

SUMÁRIO

1 INTRODUÇÃO	13
1.1 OBJETIVO GERAL	14
1.2 OBJETIVOS ESPECÍFICOS.....	14
1.3 JUSTIFICATIVA	14
1.4 ESTRUTURA DO TRABALHO	16
2 REDES WIRELESS	17
2.2 MODULAÇÃO DE SINAIS.....	18
2.2.1 Modulação de Sinal FHSS	18
2.2.2 Modulação de Sinal DSSS	19
2.2.3 Modulação de Sinal OFDM	20
2.2.4 Modulação de Sinal HR-DSSS	21
2.3 PROTOCOLOS DE FUNCIONAMENTO.....	21
2.3.1 Padrão IEEE 802.11	22
2.3.2 Padrão 802.11a	23
2.3.3 Padrão 802.11b	23
2.3.4 Padrão 802.11d	23
2.3.5 Padrão 802.11e	24
2.3.6 Padrão 802.11f	24
2.3.7 Padrão 802.11g	24
2.3.8 Padrão 802.11h	25
2.3.9 Padrão 802.11i	25
2.3.10 Padrão 802.11n	25
2.3.11 Padrão 802.11ac	25
2.4 ESTRUTURA DE CAMADAS NO PADRÃO 802.11.....	26
2.5 VULNERABILIDADES EM <i>WIRELESS</i>	26
2.6 TÉCNICAS DE INVASÃO AS REDES <i>WIRELESS</i>	28
2.6.1 Ataque de Desidentificação.....	28
2.6.2 Ataque de <i>Handshake</i>.....	29
2.6.3 Ataque Ponto de Acesso Desonesto	30
2.6.4 Ataque Homem do Meio.....	31
2.6.5 Ataque de Gêmeos Maus	32
2.6.6 Ataques de Dicionário PMKID	33

2.6.7 Ataque KRACK	34
2.7 REDES EMPRESARIAIS (ENTERPRISE)	35
3 PROTOCOLOS WIRELESS E SUAS LIMITAÇÕES	36
3.1 PROTOCOLO WEP	37
3.1.1 Protocolo WPA	39
3.1.2 Protocolo WPA2	41
3.1.3 Protocolo WPA3	43
4 ANÁLISE DE SEGURANÇA.....	47
4.1 INDOOR E OUTDOOR	48
4.2 TÉCNICAS	49
4.3 PADRÃO	50
4.3.1 Fase 1- Interações Iniciais	51
4.3.2 Fase 2- Coleta de informações.....	51
4.3.3 Fase 3- Modelagem de ameaças	51
4.3.4 Fase 4- Análise de vulnerabilidades	52
4.3.5 Fase 5- Exploração.....	52
4.3.6 Fase 6- Pós-exploração.	52
4.3.7 Fase 7- Relatório.....	53
5 TRABALHOS CORRELATOS.....	54
5.1 UM MODELO ABRANGENTE DE FLUXO DE ATAQUE E ANÁLISE DE SEGURANÇA PARA WI-FI E WPA3.....	54
5.2 SEGURANÇA EM REDES WIRELESS DOMÉSTICAS: UM ESTUDO DE CASO	55
5.3 ANÁLISE E PROPOSTA DE MELHORIA NA ESTRUTURA DE REDES SEM FIO EM ESCOLAS PÚBLICAS NA MICRORREGIÃO DE ARARANGUÁ.....	55
5.4 ANÁLISE DE PADRÕES DE SEGURANÇA EM REDES SEM FIO IEEE 802.11	56
5.5 ESTUDOS DE CASO DE SEGURANÇA EM REDES SEM FIO UTILIZANDO FERRAMENTAS PARA MONITORAMENTO E DETECÇÃO DE ATAQUES	57
6 ANÁLISE DE SEGURANÇA EM REDES WIRELESS POR MEIO DO TESTE DE PENETRAÇÃO	58
6.1 EQUIPAMENTOS UTILIZADOS.....	59
6.2 SOFTWARES UTILIZADOS.....	60
6.3 CENARIOS E MÉTRICAS UTILIAZOS PARA OS TESTES.....	61

6.4 ATAQUE DE ENGENHARIA SOCIAL	63
6.5 INÍCIO DO TESTE DE PENTESTE	64
6.6 ATAQUE EVIL TWIN	66
6.8 QUEBRANDO A PROTOCOLO WEP 64 E 128BITS	71
6.9 QUEBRANDO A CRITOGRAFIA WPA VERSÃO AES E TKIP	74
6.10 QUEBRANDO A CRITOGRAFIA WPA2 VERSÃO AES E TKIP	78
6.11 QUEBRANDO A CRITOGRAFIA WPA3	80
6.11.1 Ataque de Desautentificação.....	81
6.11.2 Ataque Krack	81
6.11.3 Ataques de Dicionário com captura do Handshake	82
6.11.4 Ataque Evil Twin.....	84
6.12 RESULTADOS OBTIDOS E DISCUSSÃO.....	86
7 CONCLUSÃO	88
REFERÊNCIAS.....	90

1 INTRODUÇÃO

Com a evolução tecnológica e a convergência das redes de nova geração, o Wireless tornou-se onipresente nos ambientes corporativos. Cada vez mais, um número maior de pessoas e de dispositivos computacionais (*smartphone, tablets, notebooks*, relógios, óculos, entre outros) adotam as redes sem fio Wi-Fi (*Wireless Fidelity*), definido pela *Institute of Electrical and Electronics Engineers* (IEEE) como padrão IEE 802.11.

Desde a implantação do padrão IEEE 802.11 em 1997 para rede local sem fio Wireless Local Area Network (WLAN), as tecnologias prosperaram para dar acessibilidade sem fio para indústrias e consumidores com alta facilidade e conveniência.

Segundo a União Internacional das Telecomunicações, órgão vinculado à Organização das Nações Unidas (ONU), em 2015, o número de internautas no mundo já era de 3,2 bilhões (G1, 2015), hoje esse número ultrapassa os 4 bilhões, segundo o serviço *online Hootsuite e We Are Social*, com destaque para o Brasil. No ano de 2018, o Brasil foi terceiro país que passou mais tempo online: foram, em média, 9h14min todos os dias (WEARESOCIAL, 2018; tradução nossa).

Com o intuito de gerar a segurança, existem atualmente, grandes empresas, visando formas de assegurar que todos tenham acesso a medidas de proteção a redes sem fio. A WI-FI ALLIANCE é uma das principais empresas, que atua nesse meio, agindo sem fins lucrativos, juntamente com outras empresas, padroniza as redes *Wireless*, sempre com muito zelo para evitar conflitos e assim tornar o Wi-Fi uma das tecnologias mais valorizadas e grandemente utilizadas no mundo.

Especificando as tecnologias e programas com relação as tecnologias *Wireless*, determina produtos que cumprem as normas de qualidade, desempenho, segurança e capacidade, para as redes *Wireless*. (WI-FI ALLIANCE, 2018, tradução nossa).

Portanto, relacionado à grande soma de pessoas conectadas e a ampla necessidade de estar sempre à frente sobre à segurança de ponta, que o presente

trabalho, estudou as tecnologias de protocolos adotados pelos roteadores Wi-Fi (WEP-WPA-WPA2-WPA3), descrevendo as melhorias obtidas com o novo protocolo WPA3 através de uma revisão bibliográfica em relação a sua antecessora WPA2.

1.1 OBJETIVO GERAL

Teste de segurança por meio de *Pentest*, para realizar a análise dos protocolos WEP, WPA e WPA2, e revisão bibliográfica da segurança do protocolo WPA3.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

- a) compreender a importância da segurança, na conexão de redes sem fio;
- b) entender e aplicar os conceitos dos tipos de protocolos WPA2 e WPA3;
- c) obter os conceitos, prática e a importância dos testes de *Pentest*;
- d) Analisar os resultados dos testes e sugerir medidas de forma a melhorar a segurança em ambientes de redes sem fio.

1.3 JUSTIFICATIVA

Manter as conexões Wi-Fi protegidas é algo necessário para assegurar os dados pessoais dos usuários, pois o número de dispositivos Wi-Fi em uso tem crescido em todo o mundo (WI-FI ALLIANCE, 2018; tradução nossa).

Todos os anos são cometidos milhões de ataques, por hackers a redes Wi-Fi. O ano de 2017 foi marcado por inúmeros ataques, estatísticas levantadas pela Norton (2018), 978 milhões de pessoas em 20 países vieram a ser afetadas pelo *cibercrime* em 2017; 44% dos consumidores foram impactados nos últimos 12 meses. Os cybercrimes mais comuns conhecidos pelos consumidores ou por alguém que eles conhecem incluem:

Tabela 1 - Estatísticas de Cybercrimes

Situação	Quantidade (%)
Dispositivo contaminado por vírus, ou ameaça de segurança	53%
Golpe de cartão de crédito ou débito	38%
Ter uma senha de conta prejudicada	34%
Obter o acesso não autorizado ou hackeamento de um e-mail ou conta de mídia social	34%
Fazer uma compra online que acabou por ser uma fraude	33%
Acessar um e-mail fraudulento ou fornecer informações privados (pessoais / financeiras) em resposta a um e-mail fraudulento	32%

Fonte: Norton, 2018

Como resultado das informações, os consumidores que foram vítimas de modo global perderam US\$ 172 bilhões - uma média de US\$ 142 por vítima – Com destaque novamente para o Brasil, que ficou em segundo lugar, com prejuízo de US\$ 22,5 bilhões (NORTON, 2018, tradução nossa).

Com base nessas situações, no ano de 2018, iniciou-se uma melhoria na linha do WPA, em roteadores sem fio, o WPA3, produzido pela *WI-FI ALLIANCE*. O protocolo de certificação de segurança WPA3 (2018) oferece algumas atualizações relevantes ao protocolo WPA2 criado em 2004.

A maior Mudança que o WPA3 apresentou foi a Autenticação Simultânea de Iguais do inglês *Simultaneous Authentication of Equals* (SAE) é uma nova forma de reconhecimento de um dispositivo que pretende se conectar a uma rede.

Uma transformação do chamado *Dragonfly Handshake* que usa protocolo para evitar que um interceptador adivinhe uma senha, a SAE estabelece exatamente como um novo dispositivo, ou usuário, deve “saudar” um roteador de rede quando eles trocam chaves criptográficas.

Evitando assim o famoso ataque conhecido como KRACK que para a série de *Handshake* fingindo perder momentaneamente a conexão com o roteador quando

de fato, ele está utilizando as possibilidades de conexão repetidas para avaliar os *Handshake* até juntar o que a senha deve ser (KOZIOL, 2018, tradução nossa).

Mais detalhes sobre o novo protocolo WPA3 será explicitada ao longo deste trabalho, mas já se pode adiantar que, essa nova atualização de segurança não dispensa a ação do usuário, o mesmo tem que sempre permanecer atento, pois a cada vez mais, técnicas de invasão são aprimoradas, e se deve levar em consideração que o protocolo de certificação de segurança WPA3, por ser algo novo pode conter falhas, podendo demorar algum tempo para oferecer a sua total funcionalidade prometida.

Segundo Koziol (2018) espera-se solucionar boa parte das vulnerabilidades existentes em um roteador Wi-Fi, e assim possibilitar ao usuário se sentir mais seguro ao navegar.

1.4 ESTRUTURA DO TRABALHO

A presente pesquisa é composta por sete capítulos, sendo o capítulo I a introdução, contendo também os objetivos e justificativa. O capítulo II introduz as redes *Wireless*, juntamente com as modulações e os padrões de funcionamento. O capítulo III trata dos protocolos e suas limitações.

No capítulo IV é onde se encontra as análises de segurança, definição e passos de como realizar os testes de *Pentest*. No capítulo V os trabalhos correlatos. No capítulo VI sendo o mais importante, pois consiste no desenvolvimento do trabalho com suas etapas e recursos necessários. E para finalizar o capítulo VII com as conclusões obtidas.

2 REDES WIRELESS

Segundo Tanenbaum (2003) conceitua “rede” como um conjunto de computadores autônomos interconectados por uma única tecnologia. Esses computadores estão interconectados por uma única tecnologia, capazes de trocar informações e partilhar recursos, interligados por um meio físico comum.

Proporcionado pela facilidade de conexão a Internet, as redes *Wireless* tem modificado de forma satisfatória o cenário de residências, escolas, escritórios, fábricas e semelhantes, se tornando cada vez mais interessante e necessário, levando em consideração que cada vez mais objetos tecnológicos em geral necessitam da conexão de rede *Wireless* para seu funcionamento.

Apresentando por sua importância especialmente pela flexibilidade e facilidade oferecida aos seus usuários. Nos dias de hoje tem-se observado um relevante aumento na quantidade de dispositivos portáteis com este tipo de suporte.

A conexão de rede *Wireless* está presente em ambientes públicos quanto em ambientes privados, empresariais, pelo fato de facilitar em grande proporção as atividades dentro da empresa. Estas redes estão cada vez mais difundidas, complementando as tradicionais áreas de redes locais (SOUZA et al., 2013). Na Figura 1 são apresentados dispositivos conectados à rede *Wireless*.

Figura 1 - Dispositivos conectados à rede Wireless



Fonte: Hadidsama (2010).

2.2 MODULAÇÃO DE SINAIS

O Padrão IEEE 802.11b trata da tecnologia sem fio (*Wireless*) focando nas redes locais sem fio do inglês WLAN que operam na faixa livre de 2.4 GHz com sua primeira e significativa evolução. Essas redes, sobretudo utilizam sinais de radiofrequência para a transmissão de dados, através de duas técnicas de modulação conhecidas como *Direct Sequence Spread Spectrum* (DSSS) e *Frequency Hopping Spread Spectrum* (FHSS), codificando dados e modulando sinais de modos diversos para equilibrar velocidade, distância e capacidade de transmissão (GARCIA, 2001).

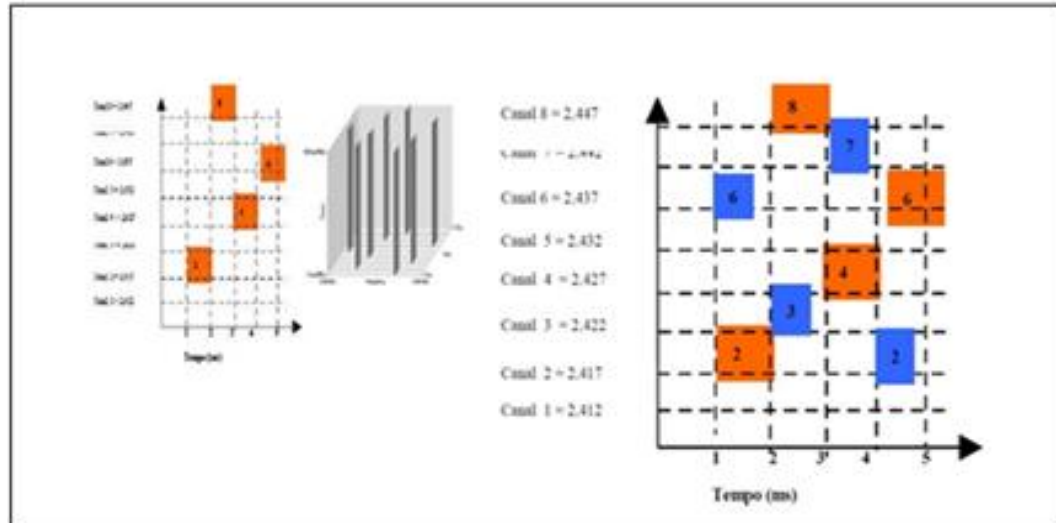
Continuando Garcia (2001) assinala que, novas tecnologias com técnicas de modulação de sinal, foram desenvolvidas em 1999, sendo elas: *Orthogonal Frequency Division Multiplexing* (OFDM) e *High Rate Direct Sequence Spread Spectrum* (HR-DSSS).

2.2.1 Modulação de Sinal FHSS

O FHSS que consiste no espectro de dispersão de saltos de frequência opera com 79 canais, cada um com 1 MHz de largura, partindo na extremidade baixa da banda ISM de 2,4 GHz. Um gerador de números pseudoaleatórios é usado para realizar a sequência de frequências dos saltos.

A partir de que todas as estações empreguem a mesma raiz para o gerador de números pseudoaleatórios e continuem sincronizadas, elas saltarão para as mesmas frequências ao mesmo tempo. Ela também proporciona certa segurança, pois um intruso que não sabe a sequência de saltos ou o tempo de parada não conseguirá espionar as transmissões, mas a sua principal desvantagem é a baixa largura de banda (TANENBAUM, 2003). Na figura 2 é demonstrado um exemplo da modulação de sinal FHSS.

Figura 2 - Modulação de Sinal FHSS

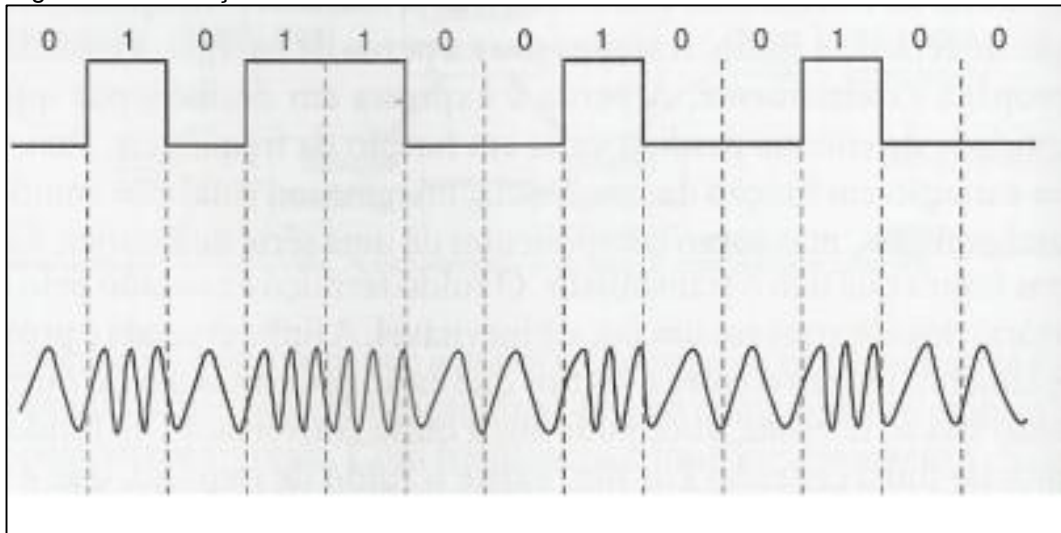


Fonte: Adaptado de Corrêa et al. (2006).

2.2.2 Modulação de Sinal DSSS

DSSS que consiste no espectro de dispersão de sequência direta, também é restrito a 1 ou 2 Mbps. Cada bit é transmitido, utilizando que atende por sequência de Barker. Ele utiliza modulação por deslocamento de fase a 1 Mbaud, transmitindo 1 bit por baud quando opera a 1 Mbps e 2 bits por baud quando opera a 2 Mbps (TANENBAUM, 2003). Na figura 3 é demonstrado um exemplo da modulação de sinal DSSS.

Figura 3 - Modulação de Sinal DSSS



Fonte: Malburg (2004).

2.2.3 Modulação de Sinal OFDM

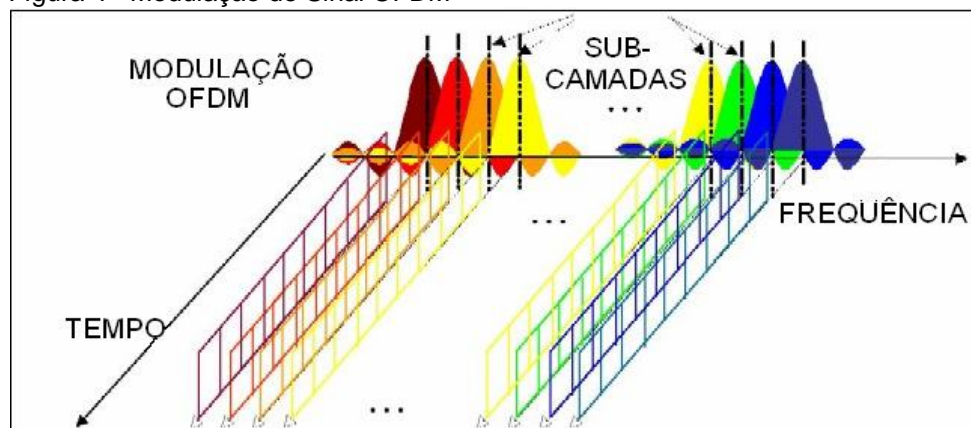
OFDM que consiste na multiplexação ortogonal por divisão de frequência, para encaminhar até 54 Mbps na banda ISM mais larga, de 5 GHz. Como são usadas diferentes frequências — 52 delas, sendo 48 para dados e 4 para sincronização — de forma equivalente ao *Asymmetric Digital Subscribe Line* (ADSL) (TANENBAUM, 2003).

Visando que as transmissões estão em várias frequências ao mesmo tempo, essa técnica é conhecida como uma forma de espectro de dispersão, mas diferente do *Code Division Multiple Access* (CDMA) e do FHSS. A parte do sinal em muitas bandas estreitas tem umas vantagens principais em relação ao uso de uma única banda larga, envolvendo melhor imunidade à interferência de banda estreita, e a possibilidade de usar bandas não adjacentes.

É utilizado um sistema de codificação complexo, baseado na modulação por deslocamento de fase, a fim de alcançar velocidades de até 18 Mbps e, na *Quadrature Amplitude Modulation* (QAM), velocidades superiores a essas. A 54 Mbps, 216 *bits* de dados são codificados em símbolos de 288 *bits*. Parte da motivação para a OFDM é a compatibilidade com o sistema europeu HiperLAN/2. A técnica tem boa eficiência de espectro em termos de *bits*/Hz e boa imunidade ao esmaecimento de vários caminhos (TANENBAUM, 2003).

Na Figura 4, é demonstrado um exemplo da modulação de sinal OFDM.

Figura 4 - Modulação de Sinal OFDM



Fonte: Adaptado de Bellardo e Savage (2003).

2.2.4 Modulação de Sinal HR-DSSS

HR-DSSS que consiste no espectro de dispersão de sequência direta de alta velocidade, é uma versão resultante da modulação DSSS, foi originada com a intenção de melhorar a velocidade de transmissão. São utilizados 11 milhões de bits para alcançar 11 Mbps na banda de 2,4 Ghz.

As taxas de dados permitidos são 1, 2, 5, 11, Mbps e podem ser adaptadas ao longo da operação para obter a melhor velocidade levando em consideração as condições atuais de carga e ruído. Esta forma de modulação é empregada no padrão IEEE 802.11b (TANENBAUM, 2003).

2.3 PROTOCOLOS DE FUNCIONAMENTO

Conforme Moreno (2016) as redes para computadores já existem há muitos anos, no entanto por não haver nem um planejamento a ser seguida, cada empresa era responsável pela produção dos mesmos, seguiam seu próprio padrão de produção, não se importando se haveria incompatibilidades.

Assim, por volta dos anos 90 os fabricantes não vendo os grandes crescimentos das redes *Wireless* no mundo, decidiram que o melhor a fazer seria criar especificações de fabricação, possibilitando assim que qualquer equipamento se comunicasse com a rede *Wireless* e também acabasse com a questão de incompatibilidades.

Com grande visibilidade no mundo todo, a IEEE foi a eleita para a criação da norma, uma vez que a mesma já havia sido a responsável pela criação da norma para redes com fio (BARBOSA, 2017).

Contudo em 1997 nasceu a normatização 802.11, com suas várias variantes que são: 802.11; 802.11a; 802.11b; 802.11d; 802.11e; 802.11f; 802.11g; 802.11h; 802.11i; 802.11n; 802.11ac. Os mesmos serão detalhados na Tabela 1.

Tabela 2 - Principais emendas do IEEE 802.11

Protocolo	Ano de Lançamento	Frequência de Transmissão-Alcance da Antena	Taxa de Transmissão-Velocidade	Modulação
802.11	1997	2.4 GHz	1 ou 2 Mbit/s	DSSS, FHSS
802.11b	1999	2.4 GHz	1, 2, 5.5, 11 Mbit/s	DSSS, CCK
802.11a	1999	3.7 ou 5 GHz	6, 9, 12, 18, 24, 36, 48, 54, Mbit/s	OFDM
802.11g	2003	2.4 GHz	Opera nos membros padrões que o 802.a 802.b	OFDM, DSSS
802.11n	2007	2.4 ou 5 GHz	150 Mbit/s (por antena)	MIMO-OFDM
802.11c	2013	5 GHz	433 Mbit/s (por antena)	UM-MIMO
802.11ad	2014	60 GHz	Opera em torno dos 6.75 Gbit/s	OFDM

Fonte: Moreno (2016).

2.3.1 Padrão IEEE 802.11

Criado em 1997 o primeiro padrão para *Wireless*, operando apenas em 1 ou 2 Mbps, uma taxa de velocidade considerada muito baixa, nesse padrão as comunicações em rede *Wireless* são realizadas via radiofrequência. O padrão 802.11 usa como método de modularização as técnicas DSSS e FHSS. A técnica DSSS partilha a frequência de operação em diversos canais e o FHSS transmite a informação em várias frequências.

Segundo Moreno (2016) de forma resumida, vai realizando saltos entre as frequências, operando com alternâncias periódicas entre elas, mas ainda que evite interferência atrasa a transmissão de dados. O padrão 802.11 utiliza o método *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) para ter acesso ao meio físico.

Dessa forma, a estação que pretende utilizar o meio físico, envia um sinal informando a todas as outras estações que vai enviar dados e por quanto tempo vai precisar ocupar o meio físico. Enquanto a estação estiver enviando dados, nenhuma outra estação pode usar o meio físico. Naquele momento o grande objetivo da primeira versão nomeada de IEEE 802.11 era determinar um padrão com os fabricantes para obter uma compatibilidade entre os dispositivos existentes (MORENO, 2016).

2.3.2 Padrão 802.11a

Concedido no fim do ano de 1999, o padrão 802.11a permite trabalhar com taxa de transmissão de dados de 6 Mb/s, 48 Mb/s e 54 Mb/s, resultando numa transmissão de 50 metros, assim regendo redes WLAN utilizando a maior frequência de 5 GHz de transmissão, sua capacidade reduz conforme o poder de penetração nos obstáculos. Suas propriedades são o crescimento de velocidade para uso em 54 Mbps ou em torno de 25 Mbps de *throughput* real (BARBOSA et al., 2017).

Opera com faixa de 5 GHz, tendo poucos concorrentes, mas o alcance é reduzido, porém com seus superiores protocolos que o 802.11b, conectando 64 clientes, contém 12 canais não sobrepostos, que possibilitam que os pontos de acessos consigam atender a área. E sua inferioridade é a incompatibilidade com o padrão 802.11b, ao qual possui uma plataforma instalada no cenário tecnológico atual. Mesmo com a taxa de transmissão maior, o padrão 802.11a não foi popular, pelo seu grande custo destinado ao mercado corporativo (BARBOSA et al., 2017).

2.3.3 Padrão 802.11b

O padrão 802.11b foi criado entre 1999 e 2001, denominado de “O Rei Dominante”, pelo feito de se popularizar, contar com a maior base instalada e possuir grandes produtos e recursos de administração acessíveis no mercado atual.

O 802.11b opera a frequência de 2.4 GHz possibilitando transmissões de até 11Mbit/s, suporta no máximo 32 clientes conectados. Este padrão está sendo substituído aos poucos pelo padrão g com maior velocidade (BARBOSA et al., 2017).

2.3.4 Padrão 802.11d

Padrão definido em 2001 e proposto como Alteração 3: Especificação para o funcionamento em domínios regulamentares adicionais. Não sendo uma especificação de nível físico tenta incluir mecanismos que possibilitem o andamento de produtos que satisfaçam a norma 802.11b (CAÇADOR, 2014).

2.3.5 Padrão 802.11e

Padrão designado como “*Media Access Control (MAC) Quality of Service (QoS) Enhancements*”, inclui funções de qualidade de serviço (QoS) para as normas 802.11a, 802.11b e 802.11g, por meio da mudança do nível MAC (CAÇADOR, 2014).

2.3.6 Padrão 802.11f

Padrão definido em 2003 e designada por “*IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation*”, que por intermédio do protocolo *Inter-Access Point Protocol* (IAPP) especifica as primitivas de serviço e protocolos que possibilitam a troca de informação entre dois Pontos de Acesso (*Access Point-AP*) de todos os fabricantes. Este protocolo é optativo, mas possibilita ao usuário a mudança de APs num sistema de *handover* (CAÇADOR, 2014).

2.3.7 Padrão 802.11g

Conforme Moreno (2016) o Padrão 802.11g é o principal utilizado no Brasil, sua vinda foi em meados de 2002 sendo compatível com o padrão 802.11b, o padrão 802.11g segue as modulações DSSS e OFDM. Por conduzir os dados numa velocidade de 54 Mbit/s, é uma versão melhorada e mais veloz que o 802.11b. Mas, se um dispositivo que suporta o padrão 802.11g (velocidade máxima de 54 Mbit/s) estiver se relacionando com um dispositivo que suporta apenas o padrão 802.11b (11 Mbit/s), a velocidade máxima alcançada por ambos será de 11 Mbit/s.

Os mesmos princípios ocorrem com a modulação de sinal: dispositivos 802.11g comunicam-se com dispositivos 802.11a via OFDM e com dispositivos 802.11b via DSSS (MORENO, 2016).

2.3.8 Padrão 802.11h

Padrão definido em 2003 e designada por “Part 11: *Wireless LAN, MAC and Physical Layer (PHY) Specifications: Spectrum and Transmit Power Management Extensions in the 5GHz band in Europe*”, apresenta o modelo de gestão dinâmica da potência de transmissão e da seleção dinâmica da frequência no exercício de dispositivos 802.11a para a Europa (CAÇADOR, 2014).

2.3.9 Padrão 802.11i

Padrão definido em 2004 e designada por “Part 11: *Wireless LAN, MAC and PHY specifications--Amendment 6: MAC Security Enhancements*”, afirma adicionar aos standards 802.11 um conjunto atual de funções de segurança, permitindo mecanismos de reconhecimento, de cifra por blocos AES (Advanced Encryption Standard) ao contrário de Rivest Cipher 4 (RC4) usando no WEP e WPA (CAÇADOR, 2014).

2.3.10 Padrão 802.11n

Padrão 802.11n, conhecido como *Word Wide Spectrum Efficiency (WWiSE)* tem como finalidade alcançar um determinado crescimento na área de cobertura de sinal, esse padrão é demasiado usado no Japão e Estados Unidos, pois nestes países a conexão residencial ultrapassa de 50 Mbit/s e transmite em 300 Mbit/s com alcance máximo de 400 metros. Operar com canais de 40 Mhz, e mantendo compatibilidade com os padrões já existentes que operam em 20 Mhz, podendo ter sua velocidade oscilando em torno de 135 Mbps (BARBOSA et al., 2017).

2.3.11 Padrão 802.11ac

O padrão 802.11ac é capaz de trabalhar com faixas de transmissão intensamente altas, em torno de 6.75 Gbit/s, isso porque essa tecnologia utiliza a

modularização MU-MIMO (*Multi-User MIMO*): cada antena transmite um valor próximo de 433 Mbit/s. Considerando três antenas, a taxa de transmissão será em torno de 1.3 Gbit/s (MORENO, 2016).

2.4 ESTRUTURA DE CAMADAS NO PADRÃO 802.11

A Figura 5 ilustra as camadas do padrão IEEE 802.11, comparando com os do modelo *Reference Model Open System Interconnection of the International Standardization Organization* (RM-OSI) (GARCIA, 2001).

Figura 5 - Estrutura de Camadas do padrão IEEE 802.11



Fonte: Garcia (2001).

2.5 VULNERABILIDADES EM WIRELESS

Por transmitir dados através do ar por meio de sinais de rádio frequência, as redes *Wireless* requerem uma maior atenção por parte de todos (usuários), pois, deve-se levar em conta que essa tecnologia se propaga num meio que não oferece garantia de segurança de alcance amplo, muito maior que as redes cabeadas (BARBOSA et al., 2017).

Considerando o avanço da tecnologia e da própria rede *Wireless*, nos quesitos desempenho e principalmente segurança, os ataques a esse modelo de rede se tornaram muito frequentes tornando-se algo infelizmente comum. Portanto junto com o avanço da tecnologia evoluíram também os ataques e programas maliciosos igualmente ou até superior.

Segundo Barbosa et al. (2017) a evolução tecnológica, o acesso à Internet e consequentemente as redes, sobretudo a *Wireless* tornou-se algo indispensável. Assim como, compras *on-line*, trabalhos *home office*, acesso a contas bancárias, entre outros serviços. Especialmente os acessos financeiros que acabam chamando a atenção de *hackers*.

O que torna ainda mais difícil manter a segurança *on-line*, é que cada vez mais equipamentos estão sendo criada para se conectarem a rede *Wireless*, consequentemente a Internet. Atualmente até mesmo eletrodomésticos estão sendo produzidos com tal função de maneira a oferecer funcionalidades extras ao usuário. Isso sem mencionar, smartphone, tablet, smartwatch e similares que estão mais conectados do que nunca (MORETTI; BELLEZI, 2014).

Com todo esse salto tecnológico, não só pessoas físicas foram afetadas, mas, também as empresas, que chamam mais atenção, tornando-se um alvo propício a invasões, por ser um local onde trafegam um grande número de dados todos os dias, indiscutivelmente e principalmente instituições financeiras.

De acordo com Moretti e Bellezi (2014) ao passar dos anos a tecnologia trouxe diversas melhorias para a vida da humanidade, principalmente na questão das redes e conexão à Internet, mas, como toda a ação tem a sua reação, também surgiram os problemas e é fundamental tomar todas as precauções cabíveis para a proteção pessoal e de dados *on-line*. Para que todo esse conjunto de ferramentas disponíveis, não se torne um problema sem solução e sim a própria solução, afinal, tudo que é bem utilizado e com boas intenções gera bons frutos e de qualidade.

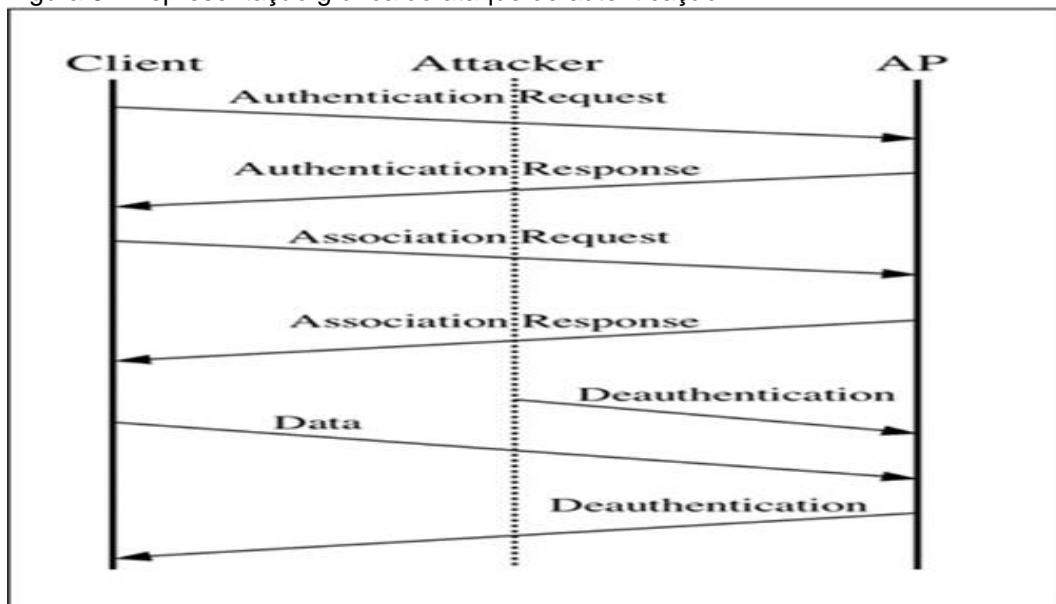
2.6 TÉCNICAS DE INVASÃO AS REDES WIRELESS

A partir desta seção do trabalho, será descrito os principais ataques que um invasor pode realizar contra um usuário/vítima em uma rede *Wireless*, para assim identificar claramente todos os pontos fracos no projeto das redes Wi-Fi de hoje.

2.6.1 Ataque de Desidentificação

O ataque de autenticação ocorre quando um cliente 802.11 seleciona um AP para usar a fim de se comunicar, ele tem o dever de primeiramente se autenticar no AP antes que a comunicação seja iniciada. Parte da estrutura de autenticação é uma mensagem que possibilita o cliente e o AP requeiram precisamente uma desautorização entre si. Lamentavelmente, essa mensagem em si não é autenticada. Consequentemente, o invasor pode falsificar essa mensagem, fingindo ser o AP ou o cliente, e direcioná-la para a outra parte, como mostra a Figura 6 (BELLARDO; SAVAGE, 2003).

Figura 6 - Representação gráfica do ataque de autenticação.



Fonte: Bellardo e Savage (2003).

Como resultado o AP ou cliente sairá do estado autenticado e recusará todos os outros pacotes até que a autenticação seja restabelecida. Quanto ao tempo que o restabelecimento necessita, depende do tempo que o cliente levará para tentar se autenticar novamente e de quaisquer *timeouts* ou *backoffs* de alto nível que possam fornecer a demanda por comunicação (BELLARDO; SAVAGE, 2003).

Ao reproduzir o ataque persistentemente, um cliente pode ser impedido de transmitir ou receber dados indefinidamente. Um dos pontos fortes desse ataque é sua grande flexibilidade: um invasor pode escolher por negar acesso a clientes individuais ou até mesmo limitar seu acesso, além de simplesmente negar serviço a todo o canal. No entanto, o cumprimento eficiente desses objetivos exige que o invasor monitore promiscuamente o canal e envie mensagens de desautenticação somente quando uma nova autenticação tiver ocorrido com sucesso que é indicada pela tentativa do cliente de associar-se ao AP.

Além disso, para evitar que um cliente "fuja" para um AP vizinho, o invasor deve verificar periodicamente todos os canais para garantir que o cliente não tenha alternado para outro ponto de acesso sobreposto (BELLARDO; SAVAGE, 2003).

2.6.2 Ataque de *Handshake*

Para um cliente se conectar a um AP, o mesmo deve primeiro ter a confiança que o cliente possui permissão para entrar na rede e dar a ele a chave que será utilizada na protocolo de dados. Esta confiança é criada e autenticada usando o *Handshake* de quatro vias. Neste protocolo, o cliente e o AP irão compartilhar determinadas informações entre si para que o outro possa criar várias chaves individualmente para chegar a um acordado de chave, a *Pairwise Transient Key* (PTK), que será a chave de sessão nova, utilizada para a transmissão segura de dados encriptados para essa ligação específica (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

A cada nova conexão feita entre o cliente e o AP, um novo PTK será criado para protocolo. Isso evita uma derivação única do PTK por um adversário para decodificação de tráfego futuro (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

A fim de realizar o ataque de dicionário off-line, o invasor irá passivamente monitorar os pacotes que vão de um cliente a um AP. Sendo que a conexão *Wireless* utiliza frequências e envia informações através do ar, um adversário pode escutar os pacotes destinados a um AP específico e obtê-los. Os únicos componentes desta troca que fazem a conexão e o PTK fresco são os *nonce* aleatórios no *Handshake*.

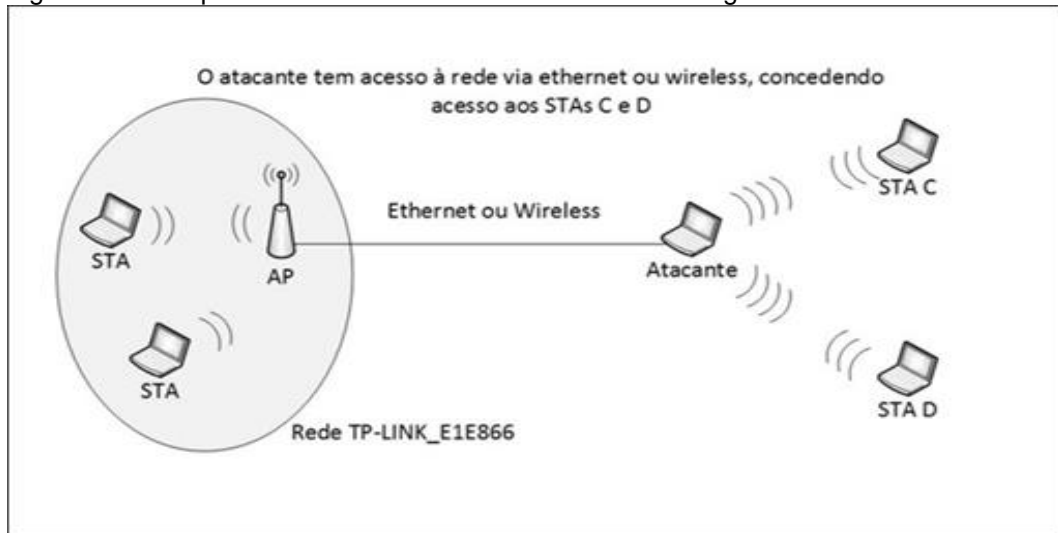
Ao capturar o *Handshake*, o invasor terá informações suficientes para testar se uma frase secreta está correta. A frase secreta candidata é usada para derivar o *Pairwise Master Key* (PMK), que é uma função de derivação de chave baseada em *Password-Based Key Derivation Function 2* (PBKDF2) do *Pre-Shared Key* (PSK), derivada da frase secreta, o *Service Set Identifier* (SSID) do AP e uma função *Hash Message Authentication Protocol* (HMAC) (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

Um PTK é criado utilizando os *nonces* que foram capturados, juntamente com todas as outras informações que permanecem constantes. A *Message Integrity Code* (MIC) é então derivada do PTK, que será verificado e comparado com o MIC capturado. Se os MICs corresponderem, isso significa que a frase secreta do candidato é correta. Este processo é repetido para cada palavra de uma lista de palavras até que a frase secreta correta seja obtida (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

2.6.3 Ataque Ponto de Acesso Desonesto

Segundo Moreno (2016) *Rogue Access Point* ou Ponto de acesso Desonesto é um ponto de acesso que está conectado a uma rede legítima e serve como uma *backdoor* para a rede *Wireless*. Assim o invasor acessa a rede legítima por meio do Rogue AP, passando por filtros de controle (como utilização de senhas WPA/WPA2 PSK da rede legítima). Por exemplo, o invasor realiza conexão à rede TP-LINK, instala um Rogue AP e emite um sinal mais forte do que a rede TP-LINK. Dessa forma, um ponto C, que antes não possuía acesso à rede TP-LINK, devido ao Rogue AP criado pelo invasor, agora tem acesso, conforme a Figura 7.

Figura 7 - A máquina do atacante está atuando como um Rogue Access Point



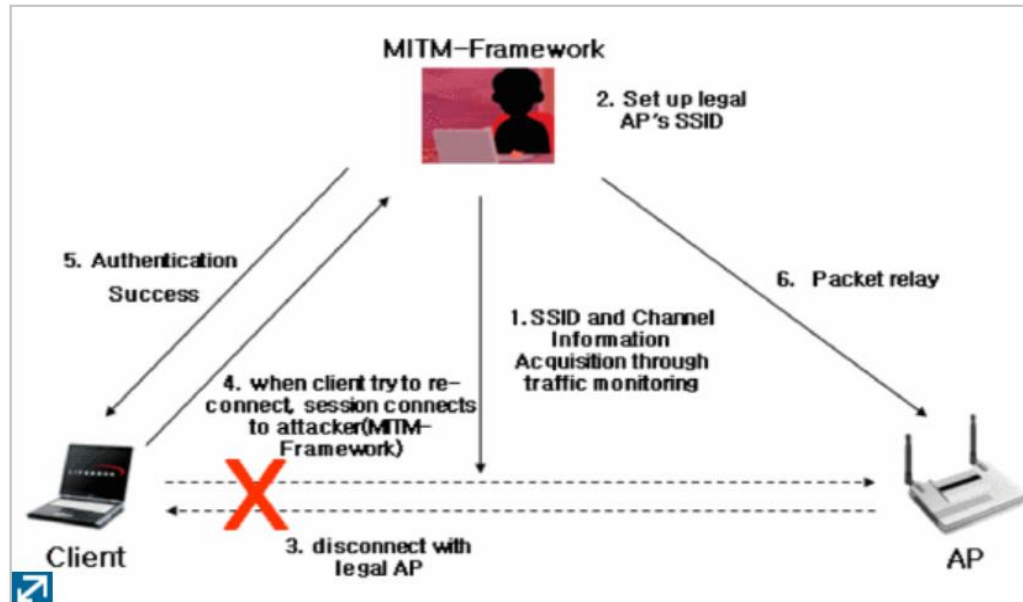
Fonte: Moreno (2016).

Para obter um Rogue AP, é necessário criar uma ponte entre a rede falsa criada com o *Airbase-ng* e a rede legítima. Considerando que um atacante esteja conectado à rede legítima, será necessário criar uma ponte entre as interfaces (MORENO, 2016).

2.6.4 Ataque Homem do Meio

O Ataque Homem do Meio do inglês *Man-in-the-Middle* (MITM) consiste no invasor conseguir ficar no meio da conexão entre o cliente e o seu destino (um AP, um site, entre outros.), capturando toda a conexão. Ataques de MITM em redes sem fio podem ser efetuados com o intuito de capturar credenciais de um usuário conforme representado na Figura 8 (HWANG et al., 2008).

Figura 8 - MITM-Fluxo do Framework



Fonte: Hwang (2008).

2.6.5 Ataque de Gêmeos Maus

Um ataque muito simples e conhecido é o *Attack-Evil Twin Attack* ou Ataque dos Gêmeos Maus que se trata de enganar o cliente para que o mesmo pense que está se conectando a um AP genuíno, quando na verdade está se conectando a um AP desonesto. O invasor imita um AP específico, na esperança de que um usuário se conecte a ele. Uma vez conectado ao AP malicioso, o invasor será um MITM e será capaz de descriptografar, visualizar e manipular o tráfego que o usuário está recebendo e enviando de seu dispositivo. O invasor encaminhará o acesso à Internet de modo que o usuário obterá o que quiser e não suspeitará de nada, mas o invasor atua como um proxy, que visualiza todos os dados em primeira mão (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

Este ataque é considerado simples devido a sua natureza (falta de autenticação). Para realizar o ataque, é necessário um roteador ou adaptador de interface sem fio em um laptop. Uma vez que tudo o que é necessário é que o SSID, o endereço MAC, o esquema de segurança e a senha sejam os mesmos para enganar o dispositivo, o invasor irá configurar o AP desonesto como tal, e posteriormente

desautenticar o usuário do AP real enviando sinalizadores de desautenticação (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

Quando o dispositivo for desconectado, ele iniciará a procura a conexão novamente. Ao escolher entre dois AP's com o mesmo SSID, a maioria dos dispositivos irá à maior parte das chances escolherem aquele com o sinal mais forte. Assim *router* alvo, contém uma frase-chave, então o invasor deve configurar o AP malicioso para ter o mesmo protocolo e a mesma frase-chave, ou nesse caso o dispositivo irá tentar usar a frase-chave lembrada para o *Handshake* e interpretá-la mal (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

2.6.6 Ataques de Dicionário PMKID

No segundo semestre de 2018 o pesquisador Jens "atom" Steube ao tentar quebrar o esquema de segurança WPA3, encontrou um novo método de ataques de dicionário *off-line* em uma rede *Wireless* foi identificado acidentalmente. Ele descreve um procedimento no qual um ataque de dicionário *off-line* consegue ser realizado sem a necessidade de capturar um *handshake* entre outro cliente e um AP (GOYAL et al., 2006, tradução nossa).

O ataque explora o elemento de informação *Robust Security Network* (RSN) de um único quadro *Extensible Authentication Protocol* (EAP) sobre LAN (EAPOL). Este quadro EAPOL é obtido na fase de autenticação da conexão diretamente antes do aperto de mão de quatro vias. Após o exame do quadro capturado utilizando uma ferramenta de captura de pacotes (por exemplo, *Wireshark*), o RSN *Pairwise Master Key Identification* (PMKID) pode ser visto na seção de dados chave WPA como um valor de *hash*. O PMKID é calculado conforme a formula (1):

$$PMKI = H(PMK, PMKName|MACAP|MACSTA) \quad (1)$$

Onde o PMK é a chave para a função e a parte de dados é um nome de PMK de cadeia fixa, o endereço MAC do AP e o endereço MAC do dispositivo que tenta ligar. Com toda essa informação conhecida, o invasor pode somente computar um PMK utilizando candidatos PSK's computados a partir de uma lista de palavras-

passa e verificar o *hash* do candidato PMKID contra o PMKID enviado no quadro EAPOL.

Se os valores corresponderem, então a tentativa de frase secreta será a frase secreta correta (KOHLIOS; HAYAJNEH, 2018; GOYAL et al., 2006, tradução nossa).

2.6.7 Ataque KRACK

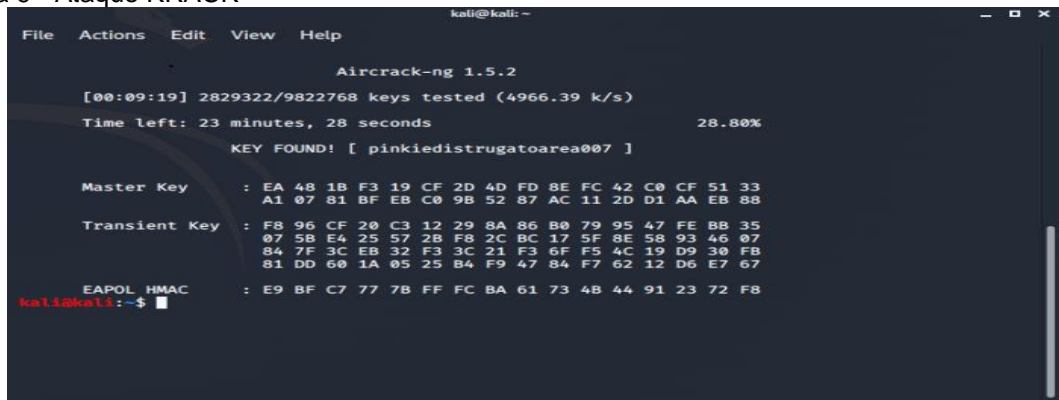
Conforme Vanhoef e Piessens (2017) encontraram uma vulnerabilidade no *Handshake* de quatro vias que daria a qualquer invasor a capacidade de descriptografar o tráfego de um usuário sem precisar capturar o *Handshake* e ter que conhecer a chave. O ataque funciona ao explorar o 4-way *Handshake* do protocolo WP2. Que é a protocolo utilizada para construir a chave para o tráfego de dados.

Nesse tipo de ataque, o invasor engana a vítima para reinstalar uma chave já em uso. E assim faz com que, alguns parâmetros associados à protocolo que asseguram o controle da comunicação são resetados (*incremental packet number* e *receive packet number*).

Tais falhas não permitem ao invasor recuperar a senha Wi-Fi, mas, sim, a descriptografar os dados sem mesmo saber a senha (VANHOEF; PIESENS, 2017, tradução nossa).

Na Figura 9 um exemplo do ataque KRACK, onde a senha foi localizada após pouco mais de 23 minutos de ataque.

Figura 9 - Ataque KRACK



```

kali@kali: ~
File Actions Edit View Help

Aircrack-ng 1.5.2

[00:09:19] 2829322/9822768 keys tested (4966.39 k/s)
Time left: 23 minutes, 28 seconds                28.80%

KEY FOUND! [ pinkiedistrugatoarea007 ]

Master Key   : EA 48 1B F3 19 CF 2D 4D FD 8E FC 42 C0 CF 51 33
              A1 07 81 BF EB C0 9B 52 87 AC 11 2D D1 AA EB 88

Transient Key : F8 96 CF 20 C3 12 29 8A 86 B0 79 95 47 FE BB 35
              07 58 E4 25 57 28 F8 2C BC 17 5F 8E 58 93 46 07
              84 7F 3C EB 32 F3 3C 21 F3 6F F5 4C 19 D9 30 FB
              81 DD 60 1A 05 25 B4 F9 47 84 F7 62 12 D6 E7 67

EAPOL HMAC   : E9 BF C7 77 7B FF FC BA 61 73 4B 44 91 23 72 F8

kali@kali:~$

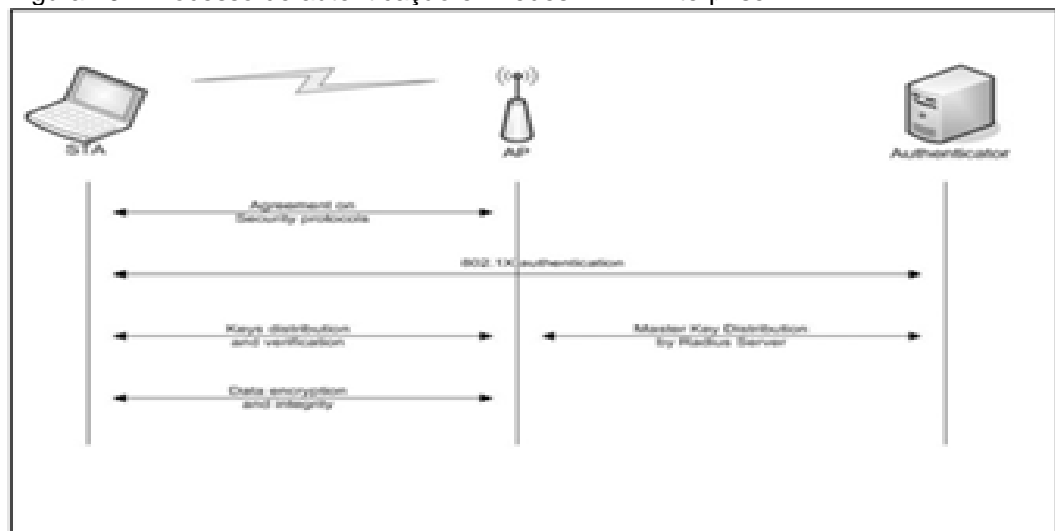
```

Fonte: Do autor.

2.7 REDES EMPRESARIAIS (*ENTERPRISE*)

Conforme demonstrado na Figura 10, a conexão em redes *Enterprise* (protocolo 802.1X) ocorre de forma similar a redes WPA/WPA2 PSK, a diferença entre o modo PMK é de responsabilidade do servidor *Radius (Authenticator)*, enquanto nas redes WPA/WPA2 PSK essa tarefa fica por conta do AP (MORENO, 2016).

Figura 10 - Processo de autenticação em redes WPA Enterprise



Fonte: Moreno (2016).

De acordo com a protocolo de autenticação selecionada, o AP e o servidor RADIUS compartilham mensagens para gerar uma chave principal. Posteriormente que uma chave principal é gerada, uma mensagem informando que a autenticação foi bem-sucedida é enviada ao AP e passada para o cliente. O AP e o cliente trocam e conferem as chaves para autenticação mútua, protocolo de mensagens e integridade de mensagens por meio de um *Handshake* de quatro vias (WEIDMAN, 2016).

Os Métodos de invasão nesse modelo de redes são similares à invasão as redes WPA/WPA2 PSK, mas o que diferencia é que enquanto nas redes WPA/WPA2 PSK, o invasor ataca diretamente o AP, nas redes empresariais o ataque é feito diretamente no próprio servidor (WEIDMAN, 2016).

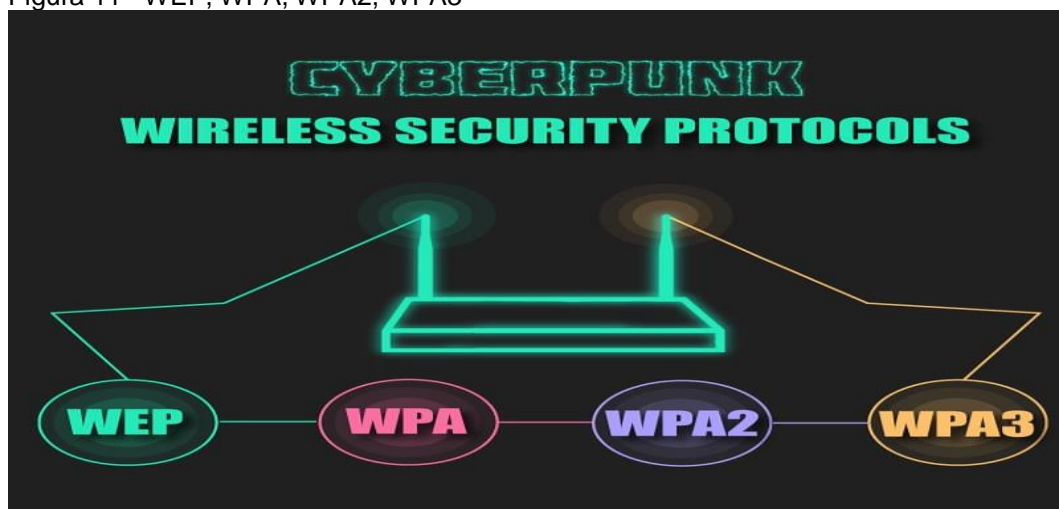
3 PROTOCOLO *WIRELESS* E SUAS LIMITAÇÕES

Segundo Zamperlini e Santos (2016) foram realizadas implementações dos protocolos para garantir maior segurança às redes *Wireless* com a forma de autenticação e encriptação, em oposição à simples distribuição de um meio sem fios à Internet. Na construção desse trabalho, o WPA2 é o protocolo mais empregado devido ao seu grande nível de segurança e tempo no mercado.

O WPA3 ainda é novo e por esse motivo não ganhou popularidade considerável, porém promete se tornar um protocolo robusto. KOHLIOS; HAYAJNEH, 2018, tradução nossa). Apesar de o WEP não seja mais adotado como um protocolo de segurança por não ser considerado seguro e sua implementação não seja mais aceita em novos dispositivos, ainda é possível ver o mesmo em poucos dispositivos nos dias atuais (ZAMPERLINI; SANTOS, 2016).

Juntamente com os benefícios de cada uma desses protocolos e métodos de protocolo, encontram-se, muitas limitações e vulnerabilidades. Os dispositivos mais recentes têm as medidas de segurança mais atualizadas e são capazes de aceitar todos os protocolos discutidos. Porém, como os dispositivos mais antigos ainda existem e são utilizados por muitas pessoas, ainda é necessário estar atento a essas limitações (ZAMPERLINI; SANTOS, 2016). Na Figura 11 são demonstrados os protocolos *Wireless*.

Figura 11 - WEP, WPA, WPA2, WPA3



Fonte: Cyberpunk (2018).

3.1 PROTOCOLO WEP

O WEP é um padrão de segurança oferecido juntamente com o padrão 802.11. O comitê 802.11 ofereceu o protocolo sabendo de seus limites, pois o WEP era a melhor opção disponível para a época. Ele foi criado com objetivo de tornar os dados trafegados tão seguros como se estivessem em uma rede *ethernet* cabeada (STANGARLIN; PRIESNTZ, 2012).

Baseando-se no algoritmo de encriptação RC4 com uma chave secreta de 40 ou 104 *bits*, concatenado com um Initialization Vector (IV) de 24 *bits* para encriptar a mensagem de texto M e a sua soma de verificação - o *Integrity Check Value* (ICV).

Conforme Lehembre (2006) a mensagem criptografada C foi definida usando a fórmula (2):

$$C = [M||ICV(M)] + [RC4(K||IV)] \quad (2)$$

O protocolo WEP não foi desenvolvida por especialistas em segurança ou protocolo, assim logo se apresentou vulnerável aos problemas RC4.

Conforme Fluhrer (2001) foi apresentado duas vulnerabilidades no algoritmo de protocolo: fraquezas não variadas e ataques IV conhecidos. Ambos os ataques são baseados no fato de que para alguns valores chave se mostra capaz que os *bytes* iniciais do fluxo chave resultem de apenas alguns *bits* da chave de protocolo (embora geralmente cada bit de um fluxo chave tenha 50% de chance de ser diferente do anterior) (LEHEMBRE, 2006, tradução nossa).

Uma vez que a chave de encriptação é desenvolvida pela concatenação da chave secreta com a IV, certos valores IV mostram chaves fracas (LEHEMBRE, 2006, tradução nossa).

As fraquezas acabaram sendo exploradas por ferramentas de segurança como o *AirSnort*, possibilitando que chaves WEP viesse sido descobertas por meio da análise de uma parte suficiente de tráfego. Além disso, se este tipo de ataque conseguisse ser desenvolvido com êxito em uma rede com alto tráfego em um período de tempo suficiente, o tempo preciso para o processamento de dados era muito longo.

Foi disponibilizado um método otimizado para o mesmo ataque, tendo em consideração não somente o primeiro byte da saída RC4, mas também o próximo resultando em uma considerável redução da quantidade de dados fundamentais para a análise (LEHEMBRE, 2006, tradução nossa).

A verificação de integridade também possui graves problemas devido ao algoritmo CRC32 empregado para este trabalho. O mesmo é geralmente aplicado para a detecção de erros, mas nunca foi visto como confiável do ponto de vista criptográfico, devido à sua linearidade (BORISOV, 2001).

Desde então, tem sido visto que o WEP fornece um nível aceitável de segurança somente para usuários domésticos e aplicações não críticas. Nos dias atuais, o WEP está definitivamente morto e não deve ser usado novamente (LEHEMBRE, 2006, tradução nossa).

Os principais problemas com relação ao WEP são relacionados à sua protocolo fraca, observando o tráfego capturado pode-se prontamente descobrir a chave usada, pois existem várias ferramentas que possibilitam decodificar os dados em poucos minutos, pois o mesmo não oferece gerenciamento de chaves e, portanto, as mesmas chaves são utilizadas por mais tempo e tende a ser de má qualidade, o padrão especificado produz suporte apenas para a chave de 40 *bits*, assim é propenso a ataques de força bruta (LESSA, 2009).

O ataque de dicionário *offline* é um tipo de ataque de força bruta onde as palavras constantemente usadas para protocolo são levadas em consideração e o resultado é comparado com para apresentar a frase-chave secreta, o vetor de inicialização é utilizado novamente e, portanto, os dados podem ser facilmente descriptografados sem o conhecimento da chave de protocolo utilizando vários métodos criptoanalíticos. O WEP não fornece segurança contra-ataques de *replay*, então, um atacante pode gravar e reproduzir pacotes e eles serão aprovados como genuínos, e quaisquer medidas de proteção contra falsificação de pacotes se torna inútil (SWATI; SHILPI, 2012, tradução nossa).

3.1.1 Protocolo WPA

A WPA foi criada em 2003 pela WI-FI ALLIANCE para solucionar os problemas na WEP. A versão 1 foi elaborada como uma solução intermediária proposta a compensar as deficiências criptográficas do WEP sem impor a aquisição de um novo *hardware* e faz utilização do *Temporal Key Integrity Protocol* (TKIP) para protocolo. A chave de 128 *bits* por pacote é criada dinamicamente para cada pacote. A PSK é uma chave estática usada para iniciar a relação entre as duas partes. Uma chave de 256 *bits* é utilizada para autenticar os dispositivos sem fio. A chave do MIC e a chave de protocolo são derivadas do PSK (KOHLIOS; HAYAJNEH, 2018).

A TKIP usa um dispositivo RC4 (implementado no *hardware* de um adaptador *Wireless*) para transformar a forma como a chave compartilhada é utilizada. O WEP usa uma chave compartilhada na protocolo, enquanto a TKIP usa uma chave compartilhada para criar outras chaves.

Conforme Kohlios e Hayajneh (2018) a TKIP fez quatro melhorias no WEP:

- a) criptografou o MIC para impedir falsificações;
- b) usou uma sequência IV específica para evitar ataques de repetição;
- c) usou a geração de chaves com melhorias;
- d) atualizou as chaves para impedir ataques de repetição de chaves.

As chaves TKIP são aplicadas depois que um cliente é autenticado e associado. Um aperto de mão de quatro vias, demonstrado na Figura 1, é feito usando as teclas TKIP, resultando em uma chave de 512 *bits* que é distribuída entre o cliente e o ponto de acesso.

Uma chave temporal de 128 *bits* e duas chaves MIC de 64 *bits* são derivadas desta chave de 512 *bits*. Uma chave MIC é para o AP à comunicação do cliente e a outra para a comunicação do cliente com o AP. O remetente de um quadro TKIP calcula o valor MIC de cada pacote de dados usando um algoritmo, chamado algoritmo Michael, que leva o MIC e uma chave privada (VANHOEF; PIESSENS, 2016).

O pacote de dados concatenado com o MIC é assim encapsulado utilizando WEP para que possa ser realizado em hardware WEP antigo. Um ICV é anexado, então o pacote é criptografado usando RC4 e uma chave que usa a função que combina a chave temporal, o endereço MAC do transmissor e o TKIP *Sequence Counter* (TSC). O receptor verificará se o TSC está em ordem e se o ICV está válido.

Se uma destas verificações não for válida, o quadro será descartado. O pacote de dados original é remontado e o valor MIC é verificado. Se for aceite, o contador de repetição TSC é atualizado (VANHOEF; PIESENS, 2016).

Têm-se muitos problemas importantes com o protocolo WPA. Um deles é o uso do mesmo algoritmo de protocolo RC4 em vez de algo superior, como o AES, e o fato de ter duas ou mais chaves RC4 computadas sob o mesmo *Initialization Vector* (IV) facilita o cálculo da *Temporal Key* (TK) por um atacante (ZAMPERLINI; SANTOS, 2016).

É vulnerável a ataques de força bruta se uma senha de baixo nível for usada. Um ataque de dicionário pode ser utilizado se a senha for menor que 20 caracteres. Outra falha do WPA é que há uma sobrecarga de desempenho maior do que o WEP. De acordo com pesquisas na área, há menor rendimento médio e maior sobrecarga quando se usa WPA-TKIP quando comparado ao rendimento e sobrecarga quando se utiliza WEP (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

A principal vulnerabilidade do WPA está no TKIP. Isto é devido a colisões de *hash* quando se utilizam funções de *hash* para misturar teclas TKIP. É fácil para um atacante calcular o TK e descryptografar qualquer pacote se duas ou mais chaves RC4 estiverem computadas sob o mesmo IV (FERREIRA, 2012, tradução nossa).

Tornando o WPA seja suscetível a riscos relacionados a colisões de *hash* ao usar funções de *hash* na mistura de teclas TKIP. Existe uma função de mistura de teclas por embalagem para descorrelacionar os IV's das teclas fracas. Um mecanismo de *re-keying* oferece novas chaves de protocolo e integridade. Esta função, chamada de chave temporal *hash*, produz uma chave de encriptação RC4 de 128 *bits*. Se um invasor coletar algumas chaves RC4 calculadas sob o mesmo IV, ele será capaz de recuperar a chave TK e a chave MIC, que é usada para identificar pacotes forjados. A maioria dos novos equipamentos que estão sendo lançados hoje não suporta uma

opção TKIP apenas. Em 2014, o TKIP foi programado para ser totalmente rejeitado. No entanto, ainda hoje existem equipamentos legados no campo que suportam e estão usando TKIP (KOHLIOS; HAYAJNEH, 2018; tradução nossa).

3.1.2 Protocolo WPA2

O WPA2 foi desenvolvido para a obtenção de um nível de segurança ainda maior que no padrão WPA (STANGARLIN; PRIESNTZ, 2012).

Assegurando que todo o equipamento com ele presente suportam 802.11i, que é um padrão para promover maior segurança na camada do MAC. Esse modo foi criado com o *Cipher Block Chaining Message Authentication Code Protocol* (CCMP). Ele utiliza a cifra de bloco AES para protocolo de dados. TKIP também está acessível para compatibilidade retroativa com *hardware* existente.

O WPA2 tem modos PSK para as redes empresariais. O IEEE 802.11 e o EAP permitem autenticação mais robusta. (SWATI; SHILPI, 2012, tradução nossa).

Devido à natureza do AES, o WPA2 precisa da mudança de *hardware* mais antigo, pois o AES tem necessidades de processamento amplo. Para criar as chaves no WPA2, o *Handshake* de quatro vias é necessário para obter uma PTK e uma *Group Temporal Key* (GTK), bem como um *Handshake* de chave de grupo para renovação do GTK ou dissociação do host (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

No início do *Handshake*, tanto o cliente como o AP têm uma PMK, que é uma função PBKDF2 do PSK, o SSID, ou nome, do AP e uma função HMAC. Depois de o cliente conduzir um pedido de ligação e o AP identificarem a solicitação o mesmo irá realizar um *nonce* (*Anonce*) e enviá-lo para o cliente. Um *nonce* é um valor aleatório que é visto pelo remetente para analisar o conteúdo que o receptor tem conhecimento sobre a informação, que está sendo transmitida através dos AP's e o cliente.

O cliente é testado utilizando-o, junto com qualquer outra informação para obter um novo valor que o AP pode analisar. Para criar o PTK, o cliente gerará seu próprio *nonce* (*Snonce*) e concatenará isso com o *Anonce*, o PMK e o endereço MAC do AP e do cliente. Parte dessa chave é usada para derivar o MIC, para assegurar que o *Snonce* lançado em texto simples não seja transformado na transmissão. Uma

vez que o AP recebe o *Snonce* e o MIC, ele irá derivar o PTK usando a mesma informação que o cliente e confirmar que o MIC coincide (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

CCMP é baseado no *Counter Mode* (CTR) com código de autenticação de mensagens *Cipher-Block Chaining* (CBC) do AES. O CTR é usado para a confidencialidade dos dados e o código de autenticação de mensagens, CBC é usado para autenticação e integridade. A protocolo CCMP recebe a chave de protocolo PTK ou GTK (se a mensagem for *unicast* ou *broadcast*, respectivamente) e a executa por meio de um algoritmo de protocolo AES em conjunto com os cabeçalhos e sinalizadores 802.11, endereço MAC do transmissor, o número do pacote da mensagem e alguns contadores que são indispensáveis para o modo contador no AES (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

O AES é um algoritmo de cifra de blocos que oferece chaves de 128-256 em sequências de 32 *bits*. A dimensão da chave e do bloco é determinada autonomamente. O valor destes blocos é substituído após o fim de cada ciclo. A chave é ampliada em 44 palavras de 32 *bits*, com cada palavra proporcionando quatro bytes. Isso cria 11 chaves para ser utilizada em 10 ciclos, a primeira das quais é usada para a inicialização do protocolo e a última usada para a inicialização da decodificação. Um número maior de rodadas é utilizado com um tamanho de chave maior.

Cada rodada consiste de uma permutação e três substituições. Este algoritmo é conhecido como seguro devido a sua complexidade proporcionada pelo tamanho da chave, bem como à complexidade das mudanças que, como já mencionado, criam em uma combinação de substituições em cada rodada (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

O principal problema do WPA2 é a obrigação de atualizar o *hardware* para implantá-lo. Essa obrigação se deve ao fato de que uma implementação CCMP e AES precisa de uma mudança no hardware atual. Todo *hardware* sendo lançado atualmente consegue suportar WPA2. O WPA2 é suportado em todos os dispositivos Wi-Fi certificados desde 2006. Mas, em redes que já foram implantadas, pode ser caro mudar todo o *hardware* por um novo que aceite CCMP e AES (SWATI; SHILPI, 2012, tradução nossa).

É de conhecimento que o WPA2 consegue ser explorado por um método conhecido como KRACK, para o qual iremos detalhar nos capítulos seguintes, desse trabalho. Um KRACK interrompe a série de *Handshake*, fingindo perder momentaneamente a conexão com o roteador. Quando de fato ele está utilizando as possibilidades de conexão repetidas para avaliar o *Handshake* até associar os caracteres que as senhas devem conter (KOZIOL, 2018).

O WPA2 também possibilita que os dados do sistema, conhecidas como quadros de gestão, sejam enviados em pacotes de texto comum do cliente para o AP. Com essa insegurança, um invasor pode alterar os pacotes para fazer parecer que os mesmos estão vindos do cliente alvo e ataques de pré-forma, como o de *authentication*. O problema está na ausência de protocolo e autenticação para manter a autenticidade das mensagens (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

3.1.3 Protocolo WPA3

Lançado em 25 de junho de 2018, o WPA3 é o mais atual sistema de segurança elaborado para reforçar a segurança em redes Wi-Fi existentes e erradicar os problemas encontrados nas versões precedentes (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

Com base na grande utilização do WPA2 durante mais de uma década, o WPA3 inclui novos recursos para facilitar a segurança Wi-Fi, proporcionar autenticação mais robusta e produzir maior força criptográfica para mercados de dados demasiado confidenciais. À medida que a indústria Wi-Fi transita para a segurança WPA3, os dispositivos WPA2 permanecerão operando e fornecendo segurança reconhecida (WI-FI ALLIANCE, 2018; tradução nossa).

A segurança WPA3 segue proporcionando ao mercado por meio de dois modos distintos de operação:

- a. WPA3-Personal - autenticação mais resiliente e baseada em senhas mesmo quando os usuários optam por senhas que não possuem as recomendações apropriadas de complexidade. O WPA3 aproveita a SAE, estabelece chaves confiáveis entre dispositivos, para produzir

proteções mais robustas para os usuários contra tentativas de adivinhação de senha por terceiros.

- b. WPA3-Enterprise - oferece o proporcional, à força criptográfica de 192 *bits*, fornecendo proteções adicionais para redes que trabalham com dados confidenciais, como governo ou finanças (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

A suíte de segurança de 192 *bits* assegura uma combinação consistente de recursos criptográficos implantadas em redes WPA3. Todas as redes WPA3 usam os recursos de segurança mais atuais não permitindo protocolos legados desatualizados e exigem o uso de *Protected Management Frameworks* (PMF) para manter a resiliência das redes de missão crítica (WI-FI ALLIANCE, 2018, tradução nossa).

Mas o que esse novo protocolo trouxe de inovador e grandioso, no quesito segurança as redes *Wireless*? A seguir se descreve as novas especificações das melhorias desse novo protocolo, que promete auxiliar, na navegação *Wireless* ou simplesmente Wi-Fi. Como já mencionado neste, o novo protocolo WPA3 utiliza o SAE (*Simultaneous Authentication of Equals*), que é novo recurso de proteção ao *Handshake*, que é elaborado para evitar ataques de dicionário no modo PSK. Ao utilizar a SAE, o WPA3 irá proteger os usuários contraprováveis tentativas de adivinhação de senha baseadas em dicionário de senhas (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

A SAE reduz a capacidade de fazer apenas um único palpite de cada vez. Toda vez que o *hacker* tentar adivinhar uma senha, ele terá que interagir "ao vivo" com o roteador, que terá as proteções necessárias embutidas para evitar adivinhações repetidas. Além disso, o uso da *Elliptic Curve Cryptography* (ECC), oferta sigilo de encaminhamento do tráfego de rede gravado. Mesmo que o invasor tenha alcançado o seu objetivo de obter a senha correta, por exemplo, através da engenharia social, ele não pode descriptografar outras sessões, pois a senha não faz mais parte do PMK. O SAE também possibilita autenticar cada ponto da conexão ao mesmo tempo e de forma independente, tornando o modo PSK muito mais seguro (BEDNARCZYK; PIOTROWSKI, 2019, tradução nossa).

A Próxima evolução da WPA3 está relacionada ao serviço PMF. Todos os dispositivos WPA3 precisam utilizar PMF. Ele melhora a segurança e a proteção da rede contra-ataques malicioso, como escutas e falsificações, passando proteção à confidencialidade das estruturas de gestão.

O terceiro novo recurso da WPA3 é o reforço da força criptográfica introduzindo a protocolo de 192 *bits*, como uma opção para o modo WPA3-*Enterprise*. Esse é um nível excessivo de segurança para, diga-se um roteador em uma rede doméstica, mas faz sentido para redes que trabalham com informações especialmente confidenciais. WPA3-*Enterprise* usará um protocolo *Galois / Counter Mode* de 256 *bits* para protocolo, um Modo de Autenticação de Mensagem *Hashed* de 384 *bits* para obter e confirmar *keys*, e uma troca *Elliptic Curve, Diffie-Hellman* e algoritmo de assinatura digital de curva elíptica para autenticar chaves (BEDNARCZYK; PIOTROWSKI, 2019, tradução nossa).

O resultado é que cada etapa do processo manterá um mínimo de protocolo de 192 *bits* para as organizações que a desejam (BEDNARCZYK; PIOTROWSKI, 2019; WI-FI ALLIANCE, 2018, tradução nossa).

Com o *Easy Connect*, que nada mais é que uma nova funcionalidade opcional, mas que veio para facilitar a vida dos usuários, em vez de incluir senhas toda vez que precisar adicionar algo a rede, os dispositivos terão códigos *QR code* exclusivos: o código para cada dispositivo funcionará como uma espécie de chave pública. Para adicionar um dispositivo, escaneia-se o código usando um *smartphone* já conectado à rede (WI-FI ALLIANCE, 2018, tradução nossa).

Após digitalizar um código QR, a rede e o dispositivo trocam e autenticam chaves para conexões subsequentes. O *Easy Connect* é um protocolo independente do WPA3: os dispositivos certificados *Easy Connect* devem ser certificados pelo WPA2, mas não obrigatoriamente certificados pelo WPA3 (KOZIOL, 2018 tradução nossa).

O *Enhanced Open* é outra novidade opcional, desta vez projetada para proteger o usuário enquanto conectado em uma rede livre. As redes livres que são, por exemplo, de cafeterias e aeroportos, apresentam um entrosamento total de problemas com os quais normalmente o usuário não se preocupa enquanto se

conecta a uma rede doméstica ou de trabalho. Muitos dos ataques que ocorrem nesse tipo de redes são ataques passivos. Com milhares de pessoas conectadas à rede, um invasor pode conseguir muitos dados se buscar e analisar os elementos que entram e saem (WI-FI ALLIANCE, 2018, tradução nossa).

O *Open Enhanced* utiliza protocolo sem fio *Opportunistic Wireless Encryption* (OWE), definida no padrão RFC 8110 da *Internet Engineering Task Force*, para proteger contra esse tipo de ataque passivo. O OWE não necessita de nenhum tipo de proteção adicional de autenticação. Ele é orientado para melhorar a protocolo de dados enviados por meio de redes públicas, para que os intrusos não consigam roubá-los. Isso também evita a chamada injeção de pacote não sofisticada, na qual um invasor tenta alterar as operações da rede, construindo e transmitindo pacotes de dados que parecem fazer parte das operações comuns da rede (WI-FI ALLIANCE, 2018, tradução nossa).

O Motivo pela qual o *Enhanced Open* não fornece qualquer proteção de autenticação é devido à natureza das redes abertas. Por padrão, elas estão disponíveis para uso geral. O *Enhanced Open* foi criado para melhorar a defesa de uma rede aberta contra-ataque passiva sem estabelecer que usuários comuns insiram senhas adicionais ou realizem etapas adicionais (BEDNARCZYK; PIOTROWSKI, 2019; KOZIOL, 2018, tradução nossa).

4 ANÁLISE DE SEGURANÇA

Conforme a Legislação Brasileira a invasão não autorizada de dispositivo informático está prevista na Lei Federal nº. 12.737/2012, a qual dispõe sobre a tipificação criminal de delitos informáticos e que alterou o artigo 154-A do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, conforme cita o artigo 2º da referida Lei Federal:

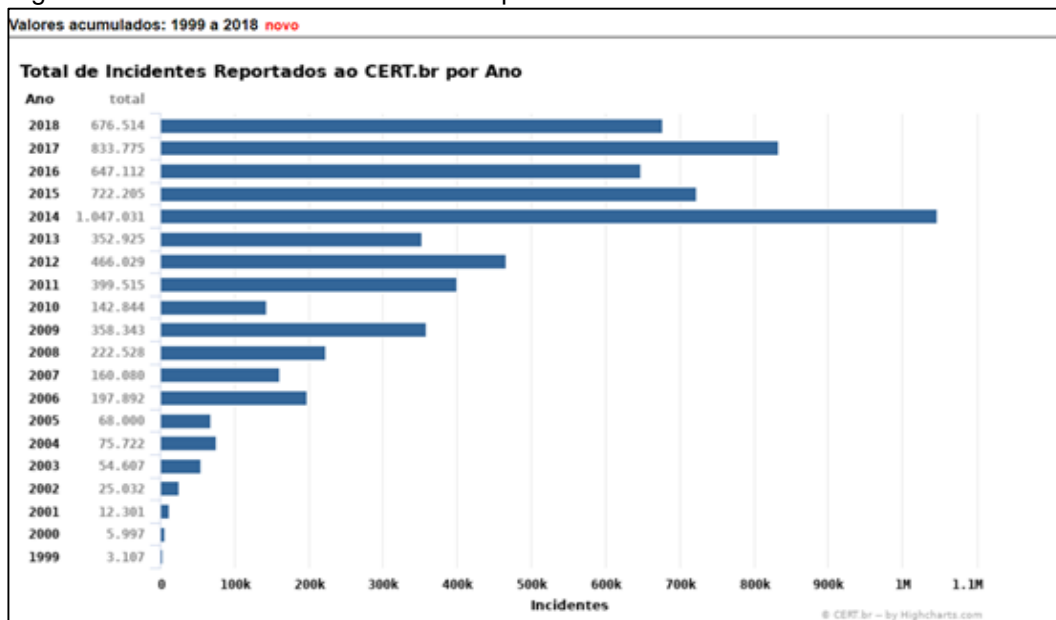
“Art. 2º.: Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012).”

Penetration Testing (Pentest) ou teste de intrusão é um processo utilizado para analisar o nível de segurança de uma determinada rede, ou melhor, avaliar as vulnerabilidades da infraestrutura de uma rede ou sistemas operacionais. O *Pentest* permite analisar a real estrutura do sistema, que é diagnosticada em todas as áreas inerentes à estrutura de segurança por um auditor. É de suma importância os testes aplicados, pois é através deles que é possível verificar as falhas em *hardware* e *software* utilizados, dependendo dos ataques, assim criar opções de defesas ou ajustes adequados (ROCHA et al, 2016).

Segundo informações do Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2018), foram registrados os seguintes ataques indevidos em computadores e redes nos últimos quatro anos: em 2015 foram 722.205 invasões; 2016 foram 647.112 invasões; 2017 foram 833.775 invasões; 2018 foram 676. 514 invasões.

É de suma importância ressaltar que existem incidentes que não são denunciados e por isso não chega ao conhecimento das autoridades responsáveis, deixando de serem incluídos nas estatísticas (ROCHA et al, 2016). Na Figura 12, é demonstrado um gráfico contendo as estatísticas dos incidentes reportados ao CERT.br entre os anos de 1999 a 2018.

Figura 12 - Estatísticas dos Incidentes Reportados ao CERT.br



Fonte: CERT.br (2018).

O objetivo do *Pentest* não é adquirir acesso não autorizado a um sistema ou servidor, somente pela diversão de se realizar um ataque virtual (hackeamento), mas sim, a partir das falhas descobertas, aplicar mecanismos adequados de segurança para o determinado sistema auditado. No final do teste será gerado um relatório com as vulnerabilidades encontradas e soluções para essas falhas.

Os mesmos tipos de teste realizados em uma auditoria consciente e autorizada também podem vir a serem feitos por criminosos virtuais (Hackers) caso isso ocorra o mesmo poderá ter acesso a informações confidenciais que comprometem a integridade dos dados (MORENO, 2016).

4.1 INDOOR E OUTDOOR

Segundo Lapesqueur e Oliveira (2012), os testes Internos ou *Indoor*, presumem que o invasor já está dentro da rede. Tais testes simulam diversos níveis de acesso à rede, tanto o de um simples usuário como o de um administrador do sistema, que representa o pior cenário possível.

A partir disso são estudadas maneiras de se ganhar privilégios e acessos adicionais. A seguir, procura-se a descoberta de vulnerabilidades que podem vir a ser

exploradas e são apresentados possíveis danos que podem ser causados, com uma conjunta análise de diferentes níveis de segurança, envolvendo controle de acesso, serviços e configurações (LEPESQUEUR; OLIVEIRA, 2012).

Os testes externos ou *Outdoor* seguem a filosofia de “Defesa em Profundidade”. Isso significa que a corporação deve apresentar toda infraestrutura (como a presença de *firewalls*) que protejam sua rede interna de acessos não autorizados. Dessa forma, o objetivo de invasão externa é ver a possibilidade de superar as defesas e obstáculos que isolam a rede interna das empresas.

Tal cenário é bem mais difícil de representar do que os testes de âmbito interno, pois a princípio não se possuía nenhuma informação da rede a ser invadida e diversas defesas devem ser superadas, como *firewalls*, *proxys*, DMZ, NAT, Sistemas de Detecção e Intrusão, entre outros (LEPESQUEUR; OLIVEIRA, 2012).

4.2 TÉCNICAS

Segundo Moreno (2016) previamente ao iniciar o processo de teste de intrusão (*Pentest*), é fundamental habituar-se ao sistema operacional que realizará a auditoria. Há inúmeras distribuições Linux que podem ser aplicadas para o teste de intrusão, como *Backtrack*, *Kali Linux*, *BackBox*, *Samurai WTF* (exclusivo para testes de intrusão *web*) e *Wifislax* (exclusivo para *Pentest* em Redes *Wireless*).

No entanto, independentemente do sistema operacional definido, o foco maior é adaptar-se com a utilização das principais ferramentas. A principal vantagem de se utilizar um sistema operacional específico para auditorias é que não há necessidade de instalar ferramentas, pois ao utilizar esses tipos de sistema, tudo que é necessário já se faz presente e pronto para uso, poupando tempo e esforços.

Conforme Moreno (2016) ao escolher a distribuição a serem utilizadas para os testes de intrusão, algumas observações preliminares precisam ser realizadas: adaptador *Wireless*, antenas e amplificadores a serem utilizados e alguns outros cuidados iniciais. Deve-se ter também atenção às placas *Wireless* que podem ser utilizadas de duas formas: monitor e modo *managed*.

O modo *managed* é o modo padrão de operação de uma placa *Wireless*: somente recebe e envia dados. O modo monitor é o que permite a escuta clandestina do tráfego de dados.

E finalmente, mas não menos importante a interface *Wireless* deve ser minuciosamente escolhida e/ou configurada, pois ao se trata de *Pentest* em redes sem fio (*Wireless*) deve-se ser escolhida uma interface compatível com os testes realizados e somente assim após coletar os dados da rede desejada, o canal da interface em modo monitor terá que ser ajustado para o mesmo canal de transmissão de dados da rede sem fio a ser auditada (MORENO, 2016).

4.3 PADRÃO

Em um ataque real, dificilmente o invasor (Hacker) irá realizar suas ações baseando-se em padrões de ataques, pois seu principal objetivo é a coleta de informações e/ou dados, em prol de seu benefício próprio, entretanto para que nenhum aspecto da segurança de uma aplicação seja negligenciado durante um *Pentest*, é necessário adotar algumas metodologias e/ou padrões que seja adequado para cada tipo de cenário. Na Figura 13 é demonstrado as fases para aplicação dos *Pentest*.

Figura 13 - Padrões/Fases para aplicação do *Pentest*



Fonte: Codevant (2017).

4.3.1 Fase 1- Interações Iniciais

Os testes de invasão têm início com a fase de preparação, que infelizmente na maioria dos casos é ignorada pelos profissionais em *Pentest* (Os chamados *Pentesters*) e até mesmo pelas empresas que solicitam o serviço, mesmo sendo algo de suma importância, pois envolve conversar com o cliente a respeito de seus objetivos para o teste de invasão, o mapeamento do escopo e assim por diante. Ao *Pentester* e o cliente chegarem a um acordo sobre o escopo, a formatação do relatório e outros assuntos, o teste de invasão propriamente dito terá início (WEIDMAN, 2016).

4.3.2 Fase 2- Coleta de informações

Na fase de coleta de informações (*information-gathering*), o *Pentester* busca por informações disponíveis publicamente sobre o cliente e destaca maneiras em potencial de conectar-se com seus sistemas (WEIDMAN, 2016).

4.3.3 Fase 3- Modelagem de ameaças

Modelagem de Ameaças é um processo utilizado para aprimorar a segurança de aplicações e redes através do reconhecimento de vulnerabilidades, em seguida, usada para estabelecer medidas para evitar ou reduzir os efeitos das ameaças em uma aplicação ou rede. Este processo é utilizado para definir onde o maior esforço deve ser empregado com o objetivo de preservar um sistema seguro.

Este é um fator que muda de acordo com as aplicações adicionadas, alteradas, removidas ou atualizadas, bem como quando os requisitos da aplicação são alterados (CODEVANT, 2018).

4.3.4 Fase 4- Análise de vulnerabilidades

O processo usado para definir e avaliar os riscos de segurança presentes no sistema é conhecido como análise de vulnerabilidade e sua aplicação é dividida em duas etapas: identificação e validação.

Na identificação, encontrar as falhas de segurança é a fundamental, neste processo é comum o uso de ferramentas de mercado ou próprias, porém apenas seu uso não é suficiente para afirmar se tal vulnerabilidade é válida, sendo assim o processo de validação, precisa-se reduzir o número de vulnerabilidades identificadas somente àquelas que são realmente válidas, por meio de testes manuais (CODEVANT, 2018).

4.3.5 Fase 5- Exploração

Na fase de exploração de falhas a utilização de um *exploit* bem sucedido, é capaz de conduzir uma fase de pós-exploração de falhas, em que se retira vantagem do resultado da exploração de falhas, de modo a descobrir informações adicionais, obter dados críticos, acessar outros sistemas e assim por diante. (WEIDMAN, 2016).

Segundo Codevant (2018) a utilização de diferentes *frameworks* e *softwares* são de grande auxílio nessa etapa. Dentre os *frameworks* e *softwares* de mercado, tem-se: Metasploit Framework, SQL Map, Canvas, Social Engineering Toolkit, Netsparker

4.3.6 Fase 6- Pós-exploração.

Nesta penúltima fase, são determinados o quão significativos são os dados obtidos e assim é trabalhar para manter o controle dos mesmos para uso posterior. Nessa fase, é de crucial importância documentar os métodos usados para a invasão (CODEVANT, 2018).

4.3.7 Fase 7- Relatório

Por fim na fase de geração de relatórios o *Pentester* sintetiza de forma aprofundada as descobertas, tanto para os profissionais executivos quanto para os técnicos (WEIDMAN, 2016).

5 TRABALHOS CORRELATOS

Com a forte utilização das redes *Wireless*, as invasões vêm sendo realizados de maneiras extremamente eficazes e com alto grau de sucesso.

Embora os métodos de defesa desenvolvidos sejam igualmente eficientes e construídos com tecnologias avançadas, infelizmente não são totalmente efetivos. Por esse motivo que cada vez mais estudos e pesquisas vêm sendo realizados nesta área.

Neste capítulo serão apresentadas algumas pesquisas relacionadas à área de segurança de rede *Wireless*.

5.1 UM MODELO ABRANGENTE DE FLUXO DE ATAQUE E ANÁLISE DE SEGURANÇA PARA WI-FI E WPA3.

Artigo apresentado para a instituição *Fordham Center for Cybersecurity* (Centro Fordham de Segurança Cibernética - FCC). Na cidade de New York, EUA no ano de 2018.

Este artigo proporciona um novo sistema de ataque que ofertar uma visão detalhada e abrangente dos possíveis ataques aos mais recentes padrões de segurança *Wireless*. Ataques existentes foram investigados, com destaque aos mais recentes, como os ataques ao *KRACK* e ao Dicionário PMKID.

A principal colaboração deste trabalho foi analisar a tecnologia ofertada no novo esquema de segurança do Wi-Fi Protected Access III (WPA3) e realizar a primeira pesquisa e a discussão abrangente de segurança a fim de determinar se o mesmo abordou as vulnerabilidades de seu antecessor. O objetivo principal de estudo do presente artigo foi alcançado através de simulações de ataques reais a AP's escolhidos para os testes.

Como conclusão foi obtida que os protocolos WEP, WPA e WPA2, mostraram suas próprias vulnerabilidades que os invasores podem explorar. Já WPA3 que é o novo esquema implementado, corrige muitos dos problemas existentes no WPA2, incluindo a desautenticação, os ataques de dicionário *off-line* e a

vulnerabilidade *KRACK*, mas não solucionou algumas das principais vulnerabilidades das redes Wi-Fi.

Porém, existem defesas e práticas seguras que podem ser adotadas como o uso de VPN para auxiliar e manter a segurança mesmo diante dessas ameaças (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

5.2 SEGURANÇA EM REDES WIRELESS DOMÉSTICAS: UM ESTUDO DE CASO

O artigo cometido para a instituição Fundação Centro de Análise, Pesquisa e Inovação Tecnológica – FUCAPI. Na cidade de Manaus/AM no ano de 2017.

Este artigo apresenta um estudo de caso com objetivo de demonstrar a necessidade de boas práticas em segurança da informação aplicadas às redes *Wireless* domésticas, por meio da análise de vulnerabilidades em redes *Wireless* localizadas em um conjunto residencial na cidade de Manaus, na qual, os procedimentos de *Pentest* e utilização das ferramentas de apoio tiveram como base a metodologia *Penetration Testing Execution Standard* (PTES) inclusive permitindo a correção das vulnerabilidades descobertas, quando autorizadas.

Como conclusão verificou-se que foram encontradas em torno de 50 vulnerabilidades baseados nas boas práticas citadas, e para conscientização dos usuários envolvidos na pesquisa, foram distribuídas cartilhas a fim de conscientizar o uso correto das redes sem fio (XAVIER; OLIVEIRA; FELEOL, 2017).

5.3 ANÁLISE E PROPOSTA DE MELHORIA NA ESTRUTURA DE REDES SEM FIO EM ESCOLAS PÚBLICAS NA MICRORREGIÃO DE ARARANGUÁ

Trabalho de conclusão de curso (TCC) realizado na Universidade Federal de Santa Catarina, para obtenção do título de Bacharel em Tecnologias da Informação e Comunicação. Na cidade de Araranguá no ano de 2017.

O presente trabalho teve como objetivo realizar um estudo das estruturas de redes *Wireless* em quatro escolas de educação básica da rede pública, situadas na microrregião de Araranguá, Santa Catarina, com objetivo de identificar problemas

e produzir a reestruturação da rede, prezando pela aplicabilidade e uso voltado para o ensino.

Após a realização da pesquisa bibliográfica, foi elaborado um estudo para definir qual seria a ferramenta que melhor se adaptaria a cada situação para realização das análises de cada escola. Levando em consideração todas as pesquisas realizadas, o estudo de caso foi a que melhor se adaptou. Para o estudo de caso, foi realizado um levantamento da estrutura encontrada juntamente com uma análise de seus equipamentos e documentação dos mesmos.

Demonstrando cada problema identificando individualmente, assim como as particularidades dos locais. Após a análise da estrutura, com o uso do software *CorelDRAW* foram desenvolvidas as plantas para cada escola, com todas as salas e um mapeamento do sinal das redes sem fio. A medição de sinal *Wireless* foi obtida com o uso de *smartphones*, que mediante a funcionalidade de conexão, pode-se demonstrar o sinal disponível em cada sala das escolas analisadas.

Com o conhecimento obtido no levantamento em relação aos aspectos técnicos, apresentou-se uma reestruturação da rede *Wireless* das escolas, alcançando os critérios de gerenciamento e segurança de rede e a distribuição de sinal *Wireless* (OLIVEIRA; BEM, 2017).

5.4 ANÁLISE DE PADRÕES DE SEGURANÇA EM REDES SEM FIO IEEE 802.11

Trabalho de conclusão de curso (TCC) realizado na Universidade do Extremo Sul Catarinense - UNESC, para obtenção do Grau de Bacharel em Ciência da Computação. Na cidade de Criciúma no ano de 2009.

O presente trabalho visa ter como objetivo realizar um estudo sobre a análise e padrões dos protocolos das redes sem fio WEP, WPA e WPA2 para obter a possibilidade de avaliar o seu grau de vulnerabilidades dentro do padrão 802.11, tendo em vista que os mesmos possuem falhas de implementação e na forma de utilização.

Como conclusão do presente trabalho, observou-se que o protocolo WEP, apresenta a maior vulnerabilidade comparada aos outros, independentemente do tamanho da chave 64 ou 128 *bits* e da senha utilizada, o mesmo apresenta um nível

de segurança fraco. Sendo assim o uso desse protocolo criptográfico deve ser evitado sempre que possível.

No que se trata dos protocolos WPA e WPA2, observou-se que possuem uma segurança de maior qualidade, se comparado ao WEP, porém nem todas as vulnerabilidades foram sanadas de forma satisfatória (COSTA, 2009).

5.5 ESTUDOS DE CASO DE SEGURANÇA EM REDES SEM FIO UTILIZANDO FERRAMENTAS PARA MONITORAMENTO E DETECÇÃO DE ATAQUES

Trabalho de conclusão de curso (TCC) realizado na Universidade do Extremo Sul Catarinense - UNESC, para obtenção do Grau de Bacharel em Ciência da Computação. Na cidade de Criciúma no ano de 2011.

O Presente trabalho visa discutir os conceitos de redes sem fio, métodos de segurança, vulnerabilidades e alguns ataques existentes. Utilizando estes conceitos, é realizado um teste de eficiência no monitoramento e detecção de ataques, fazendo utilização de ferramentas de código aberto para Linux, *Kismet* e *Beholder*. Como conclusão foi obtida através dos testes produzidos com estas ferramentas a importância sobre a segurança e do monitoramento dos pontos de redes sem fio (CARLESSI, 2011).

6 ANÁLISE DE SEGURANÇA EM REDES WIRELESS POR MEIO DO TESTE DE PENETRAÇÃO

Para elaboração do presente trabalho, foi realizado um amplo estudo inicialmente em artigos e livros sobre redes sem fio, e principalmente sobre *Pentest*, a fim de obter conhecimento sobre os assuntos abordados e assim poder realizar os testes de com sucesso, sendo os mesmos o grande objetivo da presente pesquisa.

Posteriormente foram executados os primeiros testes de Pentest de nível básico nos protocolos WEP, WPA, WPA2 a fim de se certificar que os testes de alto nível seriam realizados com sucesso.

Foram elaborados três cenários com diferentes APs, para realização dos testes, e utilizado vários formatos de testes com suas devidas métricas, e em seguida a coleta de dados, para pôr fim poder realizar conclusão e identificar as melhorias entre o protocolo WPA2 e seu sucessor o WPA3.

Infelizmente uma das dificuldades encontradas para realização do presente trabalho foi não conseguir acesso a um AP com o protocolo WPA3, mesmo tendo sido pesquisado em várias lojas on-line e consultado todos os distribuidores de AP's no Brasil.

Outro empecilho foi dado a atual condição mundial, com a pandemia do Covid-19 atenuada com a alta do dólar, que impossibilitou a importação de um AP com o protocolo WPA3.

Ao todo foram realizados quatro testes de Pentest com os protocolos WEP, WPA e WPA2, já o protocolo WPA3 teve seus resultados obtidos a partir de artigos científicos que já realizaram os mesmos testes pretendidos neste trabalho. Adiante será abordado a fundo os equipamentos, cenários, *software* e os testes realizados detalhadamente com cada protocolo.

6.1 EQUIPAMENTOS UTILIZADOS

Para realização dos testes de Pentest com os protocolos WEP, WPA, WPA2 foram utilizados três tipos de AP's diferentes. No Quadro 1 é definido a marca, modelo e versão de cada um.

Quadro 1 - AP's utilizados

Marca	Modelo	Versão
TP-Link	TL-WR841HP	Ver 2.0
	TL-WR740N	Ver:4.23
	TL-WR849N	Ver:6.0

Fonte: Do autor.

A fim de simular o atacante, foi utilizado um notebook DELL, modelo 7460 com auxílio de uma placa *Wireless* USB 2.0 modelo 802.11N, e da parte contrária, ou seja, a vítima um *Smartphone Xiaomi* modelo MI9. No Quadro 2 é tratado as especificações dos equipamentos.

Quadro 2 - Especificações dos Equipamentos

Notebook Dell Modelo: 7460	Processador Intel Core i7-7500U de sétima geração (até 3.5 GHz) Cache 4M
	Tela 14 Polegadas LED Full HD
	Memória RAM 8 GB tipo DDR4 – 2133MHz
	Armazenamento HD de 1 TB
	Placa de vídeo dedicada NVIDIA GeForce 940MX com 4GB do tipo GDDR5
	Sistema Operacional Kali Linux
	Comunicação: Rede 10/100 RJ-45 Ethernet network Wireless802.11ac
Smartphone Xiaomi Modelo: MI9	Sistema Operacional Android MIUI 12
	Armazenamento 128 GB
	Memória RAM 6 GB
	Tecnologia sem fio Bluetooth, 4G, Wireless, NFC, GPS
	Tamanho da tela 6.39 polegadas, Super AMOLED
	Bateria 3300 mAh
	Cor Azul

Fonte: Do autor.

6.2 SOFTWARES UTILIZADOS

O sistema operacional ou somente SO utilizado foi o Kali Linux em sua versão 2020.1 o mesmo foi adotado por ser de utilização livre, e principalmente por ser uma distribuição Linux especialmente voltada Pentest, que inclusive é uma das mais utilizada em todo o mundo por profissionais da área, trazendo consigo todos os softwares necessários para a realização dos testes deste trabalho.

É importante ressaltar que o SO foi utilizado por meio de uma Live USB, pois além desse método ser de mais fácil utilização, vários profissionais da área de Pentest recomendam esse tipo de utilização por essa distribuição Linux não ser para de uso doméstico e necessitar de atualizações constantes para sua utilização.

Já os softwares utilizados foram *Wash*, *Bully* e o *Aircrack-NG*, composto por vários outros *softwares*, que são eles: *Airmon-NG*, *Airodump-NG*, *Aireplay-NG* e *Airbase-NG*, trata-se de uma suíte de ferramentas que realiza vários testes, sendo também utilizada em diferentes áreas de segurança de redes *Wireless*, como monitorização de pacotes, ataque, testes e *cracking*. (CIFUENTES; GATICA; LINFATI, 2017, tradução nossa).

Esses Softwares são encontrados somente em distribuições Linux, por necessitar de linhas de comandos para serem executados e o mais importante necessita que o usuário seja administrador geral do sistema, ou seja, usuário root. No Quadro 3 será listado em formato de tabela os *softwares*, com suas respectivas funcionalidades.

Quadro 3 - Programas Utilizados

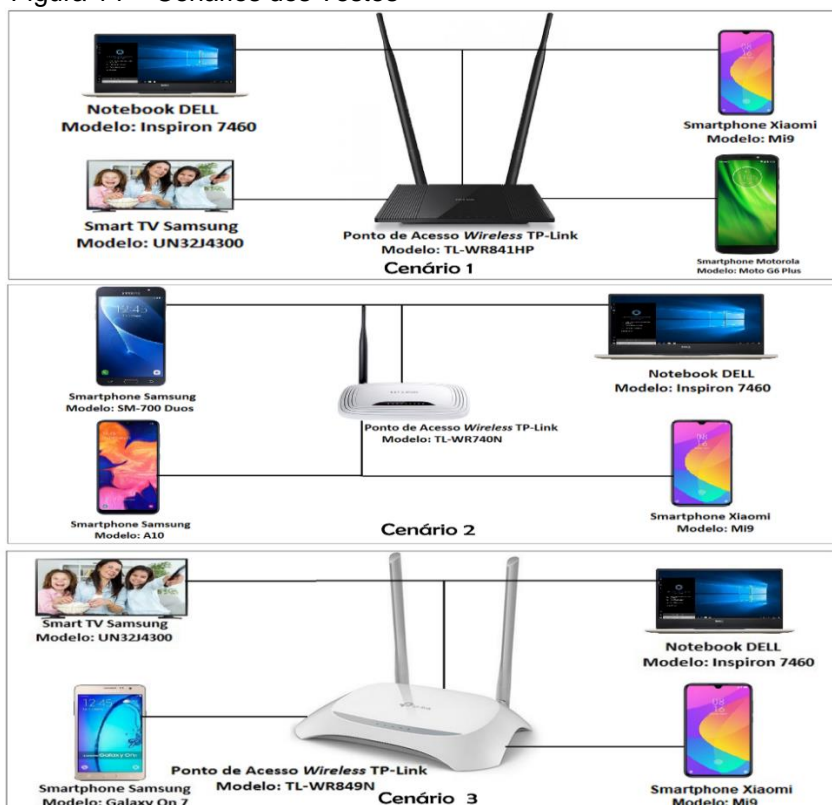
Softwares Utilizados	
Ferramenta	Funcionalidade
Wash	Realiza o monitoramento da rede Wireless para detecção de APs com o protocolo WPS ativo.
Bully	Realiza o ataque de força bruta contra o protocolo WPS.
Aircrack-NG	Realiza o ataque de força bruta contra as chaves.
Airmon-NG	Habilita a função modo monitor na interface wireless
Airodump-NG	Monitora os pacotes, e reporta as redes próximas.
Aireplay-NG	Envia pacotes ao AP, mas também pode ser utilizado para a geração de tráfego ARP, pois assim há um aumento no tráfego de pacotes, diminuindo o tempo necessário para a quebra das chaves. Outra função desempenhada é o ataque de desautentificação, que desconecta o usuário temporariamente.
Airbase-NG	Realiza vários ataques direcionados ao cliente, em vez de ataques do AP; como a criação de pontos de acesso falsos/ Evil Twin.

Fonte: Adaptado de Couto (2018).

6.3 CENARIOS E MÉTRICAS UTILIZADOS PARA OS TESTES

As métricas definidas para os testes foram a utilização de três AP's de modelos diferentes como já mencionado, alterando também os locais, para que os cenários diferenciassem o máximo possível e comprovassem a eficácia e autenticidade dos testes. Como é ilustrado na Figura 15.

Figura 14 - Cenários dos Testes



Fonte: Do autor.

Para execução do presente trabalho foram escolhidos os testes de Pentest, mais robustos e mencionados nas bibliografias, que são eles Engenharia Social, Dicionário de Senhas com auxílio da captura do *Handshak*, *KRACK*, ataque ao WPS e o *Evil Twin*.

Foram utilizadas os protocolos WEP alternando entre sua versão 64bits e 128bits, WPA e WPA2 alternando entre suas versões AES e TKIP e a manipulação de chaves. Com relação às chaves foram utilizadas, tendo como base a *Wordlist Rockyou* que nada mais é que um dicionário de senhas essencialmente necessário para a execução de um dos testes escolhidos, com os mencionados protocolos. Pôr padrão a *Wordlist Rockyou* é trazida juntamente com o *Kali Linux*, e mesmo tendo a possibilidade de se utilizar outros tipos de dicionário de senhas mais complexos e robustos, a utilizada se mostrou de grande eficácia.

Já o protocolo WEP teve as chaves escolhidas pelo próprio autor, tendo em vista que não há necessita de um dicionário de senhas para ser testada.

Nos protocolos WEP e WPA foram utilizadas dez tipos de chaves com complexidade diferentes, já para o protocolo WPA2, quinze tipos de chaves com complexidade diferentes foram utilizadas, essa última foi considerado realizar uma quantidade de testes maior, pois é um dos protocolos foco do presente trabalho. Ao todo em todos os AP foram executados 39 testes, somando 117 no seu todo, que serão abordados detalhadamente ao decorrer dos próximos capítulos.

Uma das métricas também definidas foi à análise dos pacotes que trafegavam pela rede em cada teste, utilizando o modo monitor da placa Wireless, a fim de coletar todas as informações necessárias para a execução dos mesmos. E por fim a realização das configurações adequadas em todos os AP, a fim de tentar trazer mais segurança em sua utilização, baseando-se nos testes de Pentest realizados, configurações essas que serão detalhadas também nos próximos capítulos.

6.4 ATAQUE DE ENGENHARIA SOCIAL

O primeiro teste iniciado foi o de Engenharia Social, que consiste em uma conversa com ambos os donos dos AP's, induzindo os mesmos a entregar as credencias do seu AP, como tipo de protocolo adotada e senha.

Foi empregado o seguinte questionário: Para que você utiliza sua rede Wireless? Como você utiliza sua Rede Wireless? e Qual senha de acesso a sua rede Wireless?

Nas duas primeiras perguntas as respostas foram sempre as mesmas como acessar a internet, ver Netflix, Youtube dentre outros. Já com relação a senha a mesma foi obtida com sucesso em todas as conversas, o que levou a perceber que dias atuais é comum não dar a devida importância ao passar esses tipos de dados a outras pessoas, principalmente quando se trata de pessoas que entendem pouco ou não são da área computacional.

A situação se agrava, ao ver que na maioria dos casos as configurações do AP são deixadas como padrão de fabrica como *Login* e Senha administrativa, para acesso ao dispositivo, função WPS ativado dentre outras.

Ao final da conversa, foram explicados aos donos dos AP's, quais são os perigos de fornecer esses tipos de dados a qualquer pessoa, e quais as medidas tomar ao cair nesse erro, ou quando há a necessidade de passar os mesmos, como por exemplo, modifica a senha de acesso a rede *Wireless*.

6.5 INÍCIO DO TESTE DE PENTESTE

Como já mencionado anteriormente, para desenvolvimento do presente trabalho foram realizados testes de Pentest com três AP's diferentes, em seus protocolos: WEP alternando entre sua versão 64bits e 128bits, WPA e WPA2 alternando entre suas versões AES e TKIP. Tendo em vista que para ambos os testes, o início dos *Pentest* são os mesmos, essa parte inicial será descrita a seguir e posteriormente tratada as particularidades de cada uma.

Para início dos testes, após definir o tipo de protocolo a ser utilizado juntamente com sua senha, se faz necessário também preparar o SO, com o comando `sudo airmon-ng check kill` utilizado para interromper qualquer processo, que possa impedir que a placa *Wireless* entre em modo monitor.

Em seguida é chegado a hora de iniciar a placa *Wireless* em modo monitor, para isso é utilizado a ferramenta *Airmon-NG*, pertencente a suíte *Aircrack-ng*. O modo monitor é inicializado com o comando `sudo airmon-ng start wlan0`, como demonstra a Figura 15.

Figura 15 - Preparação do Sistema Operacional

```

kali@kali: ~$ sudo airmon-ng check kill
Killing these processes:
  PID Name
  1243 wpa_supplicant
kali@kali: ~$ sudo airmon-ng start wlan0

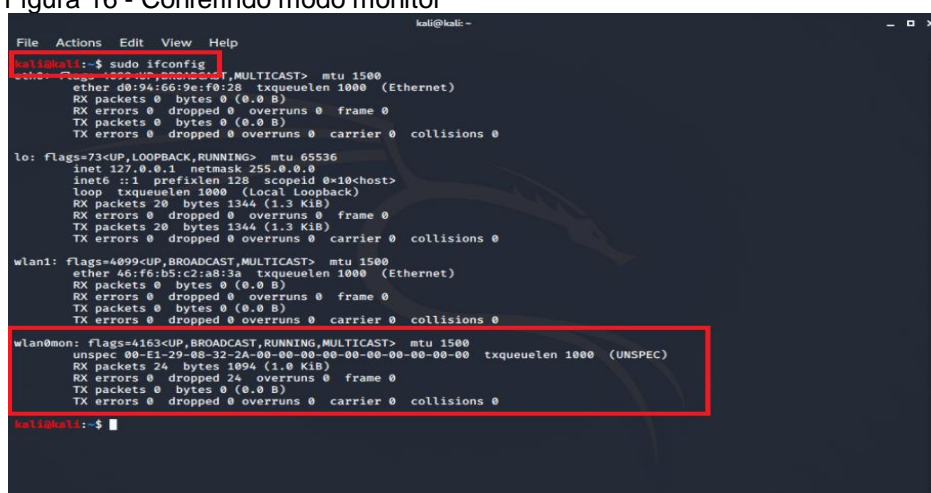
PHY      Interface  Driver      Chipset
phy0     wlan0      mt7601u     Ralink Technology, Corp. MT7601U
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
phy1     wlan1      ath10k_pci  Qualcomm Atheros QCA6174 802.11ac Wireless Network Adapter (rev 32)
kali@kali: ~$

```

Fonte: Do autor.

Mesmo não sendo necessário, é recomendado verificar que a placa *Wireless* entrou em modo monitor com sucesso, e para executar essa verificação se faz uso do comando *sudo ifconfig*. Nota-se que na Figura 16 que a denominação *wlan0* foi alterada para *wlan0mon*, comprovando assim que a placa *Wireless* entrou em modo monitor.

Figura 16 - Conferindo modo monitor



```

kali@kali: ~$ sudo ifconfig
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether d0:94:66:9e:f0:28 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10chost>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1344 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1344 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 46:f6:b5:c2:a8:3a txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    unspec 08:e1:29:08:32:2a-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
    RX packets 24 bytes 1094 (1.0 KiB)
    RX errors 0 dropped 24 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali: ~$
  
```

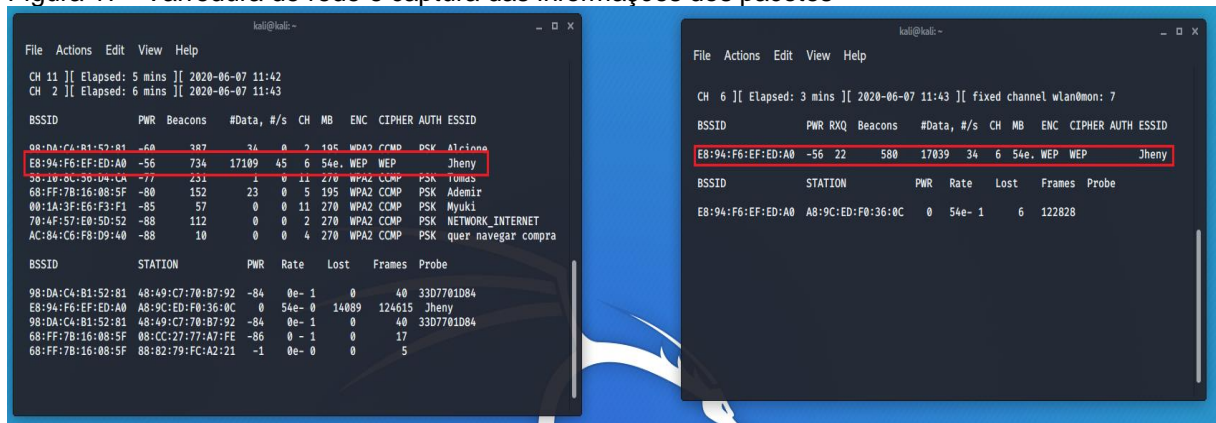
Fonte: Do autor.

Tendo finalizado toda a preparação descrita, é chegada a hora de iniciar o teste. Com a abertura de um novo terminal e fazendo o uso da ferramenta *Airodump-NG*, também pertencente à suíte *Aircrack-NG*, executa-se o comando *sudo airodump-ng wlan0mon*, com ele é possível realizar uma varredura e localizar as redes *Wireless* próximas, juntamente com algumas informações importantes de cada rede como: o nome da rede, endereço BSSID, endereço MAC, o canal que está utilizado, o tipo de protocolo adotado e os clientes a cada conectado.

Após escolher o alvo, e obter as informações necessárias, se faz necessário a abertura de um novo terminal e a reutilização da ferramenta *Airodump-ng*, para que seja possível capturar as informações dos pacotes que trafegam pela rede alvo e grava-las em um arquivo que será de fundamental auxílio na obtenção dos resultados esperados.

Na execução dessa etapa do teste se faz a utilização do comando `sudo airodump-ng -c 6 --bssid E8:94:F6:EF:ED:A0 -w WEP_1 wlan0mon`. O parâmetro (-c 6), se trata do canal em que a rede está operando, o parâmetro (--bssid E8:94:F6:EF:ED:A0) se trata do endereço BSSID, já o parâmetro (-w WEP_1), é o nome do arquivo que com já mencionado, é responsável por coletar informações dos pacotes que trafegam pela rede, e que pode ser receber qualquer nome. A Figura 17 demonstra com mais detalhes as últimas etapas.

Figura 17 - Varredura de rede e captura das informações dos pacotes



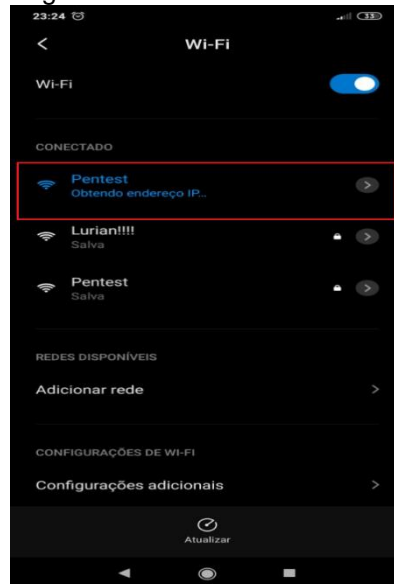
Fonte: Do autor.

6.6 ATAQUE EVIL TWIN

Foi realizado um total de 9 testes, sendo 3 em cada AP com cada protocolo, o Ataque Evil Twin, tem como objetivo a criação de um AP com os mesmos dados do AP alvo, a fim de levar os clientes que estavam conectados ao AP verdadeiro, se conectarem ao falso.

Após realizar as etapas do subcapítulo 6.5, é necessário utilizar a ferramenta *Airbase-NG*, que como já descrito pertence à suíte *Aircrack-ng*, e tem como função vários tipos de ataques incluído o de ponto de acesso falso, executando o comando `sudo airbase-NG -c 4 -e Pentest -a 18:A6:F7:C9:11:26 wlan0mon`, em um novo terminal. Tendo realizado essa etapa o sinal do ponto de acesso falso já é apresentado, como demonstra a Figura 18.

Figura 18 - AP falso



Fonte: Do autor.

Para concluir o ataque, é necessário que as vítimas se conectem ao mesmo, e para isso são induzidas a se desconectarem do seu AP verdadeiro com um ataque de desautenticação, utilizando a ferramenta *Aireplay-NG* como na Figura 19, que como já mencionado possui diversas funções, incluindo o presente ataque de desautenticação, com o novo terminal executa-se o seguinte comando: `sudo aireplay-ng -0 5 -a 18:A6:F7:C9:11:26 wlan0mon`.

Figura 19 - Ataque de Desautenticação

```
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ sudo aireplay-ng wlan0mon -0 5 -a 18:A6:F7:C9:11:26
22:58:44 Waiting for beacon frame (BSSID: 18:A6:F7:C9:11:26) on channel 9
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:58:44 Sending DeAuth (code 7) to broadcast -- BSSID: [18:A6:F7:C9:11:26]
22:58:45 Sending DeAuth (code 7) to broadcast -- BSSID: [18:A6:F7:C9:11:26]
22:58:45 Sending DeAuth (code 7) to broadcast -- BSSID: [18:A6:F7:C9:11:26]
22:58:46 Sending DeAuth (code 7) to broadcast -- BSSID: [18:A6:F7:C9:11:26]
22:58:46 Sending DeAuth (code 7) to broadcast -- BSSID: [18:A6:F7:C9:11:26]
kali@kali:~$
```

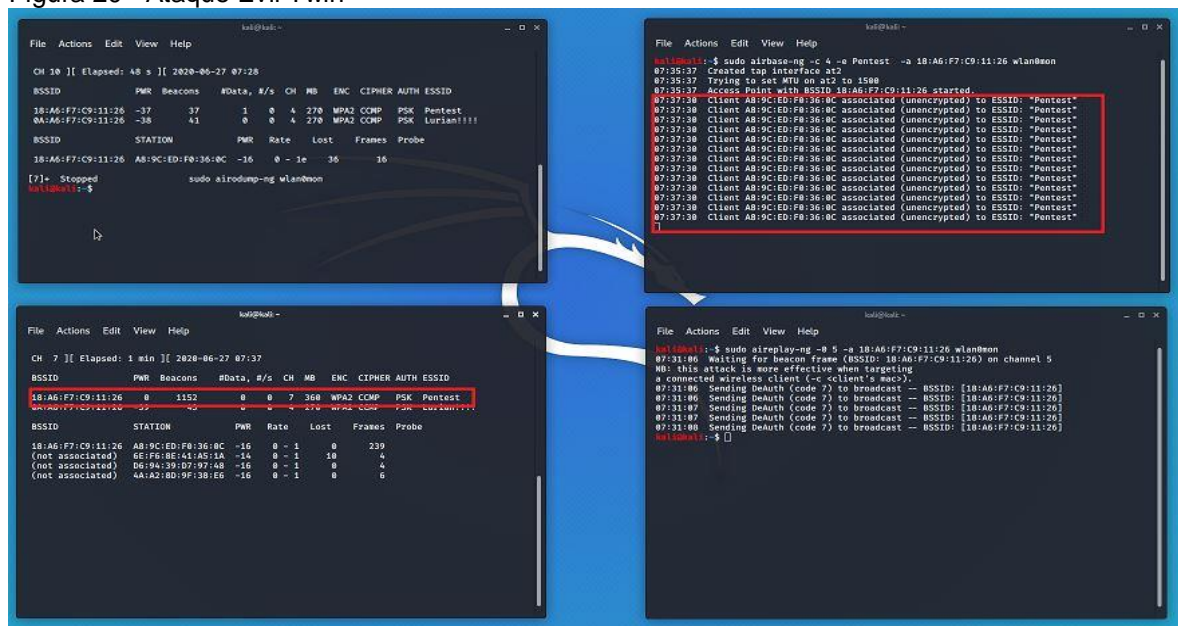
Fonte: Do autor.

Com relação ao comando, o parâmetro (-0) indica a função de desautenticação da ferramenta *Airplay-NG*, o parâmetro (5) se refere à quantidade de ataques de desautenticação que são enviadas ao AP e por último o parâmetro (-a 0C:80:63:97:F3:C0) é o endereço BSSID do AP alvo.

Possibilitando que momentaneamente os clientes conectados ao AP verdadeiro, se desconectem e reconectem automaticamente, pois ao fazer isso tendo em vista que o sinal do AP falso é mais forte e está em modo OPEN, se conectem ao AP falso.

Após realizar o ataque de desautenticação, é possível observar no segundo terminal, através da Figura 20 que a conexão dos clientes ao AP falso ocorreu como esperado, obtendo assim sucesso no teste de Pentest.

Figura 20 - Ataque Evil Twin



Fonte: Do autor.

6.7 Ataque WPS

O WPS é um protocolo que foi lançado e introduzido em 2007 pela Wi-Fi Alliance para conceder o emparelhamento seguro de dispositivos Wi-Fi com AP's compatíveis. O WPS possui dois métodos principais, o método baseado em PIN com oito dígitos e a *Push Button Configuration* (PBC), na qual um botão físico necessita ser pressionado no AP.

O método baseado em PIN é obrigatório para todos os dispositivos certificados WPS, já o PBC é opcional para os clientes sem fio, mas obrigatório para os APs. Em dezembro de 2011, Stefan Viehböck descobriu uma grande falha de segurança no protocolo WPS. Essa falha torna prático um ataque de força bruta nos APs. (SANATINIA et al., 2013, tradução nossa)

Ao descobrir as vulnerabilidades do protocolo WPS os fabricantes dos APs decidiram incorporar firmwares, para evitar ataques de força bruta. Assim se o código PIN for digitado incorretamente várias vezes o mesmo é bloqueado automaticamente, até que seja reiniciado o AP.

Já outros fabricantes desabilitaram diretamente a opção WPS por meio do código PIN, sendo somente possível aciona-lo pelo PBC. (MILLS, 2019)

Mesmo levando em consideração a informação, foram realizados os testes com o protocolo WPS com todos os AP, a fim de verificar as vulnerabilidades do mesmo, e se realmente os firmwares realizam a sua proteção. Para realização dos testes de Pentest com o WPS, após realizar as etapas do subcapítulo 6.5, porem especialmente nesse Pentest fica a critério efetuar a captura de pacotes, é utilizado a ferramenta *Wash* como demonstra a figura 21, responsável por fazer a varredura e localizar as redes *Wireless* próximas com o protocolo WPS ativo, o comando para utilização da ferramenta é *sudo wash -i*, em alguns casos um erro de falta de pacotes pode vir a ocorrer, mas o mesmo pode ser corrigido adicionando o parâmetro *(-C)* ao comando, ou seja *sudo wash -i -C*.

É possível observar na imagem 22, que no segundo terminal é apresentado a seguinte mensagem: *WPS lockout reported* e para reforçar uma nova varredura com o *software Wash* foi realizada, e como é mostrado no terceiro terminal o protocolo WPS encontra-se bloqueado.

Isso ocorreu, pois como já mencionado os fabricantes dos AP's decidiram incorporar firmwares, para evitar ataques de força bruta ao protocolo WPS, sendo assim com os resultados obtidos com o presente teste foi possível demonstrar a eficácia desses *firmwares*, impossibilitando a obtenção do PIN do protocolo WPS e consequentemente da senha do AP alvo.

6.8 QUEBRANDO O PROTOCOLO WEP 64 E 128BITS

Contando com um total de 30 testes, o tipo de *Pentest* escolhido para o presente protocolo foi o ataque *KRACK*, para dar início ao teste é definido o tipo de protocolo WEP sua versão (64 ou 128bits) e senha da mesma no AP, como demonstra a Figura 23 e 24. O que difere um protocolo do outro, é que a WEP-128bits permite chaves mais robustas, que incluam números e caracteres especiais.

Figura 23 - Definição do protocolo WEP versão 64bits e senha no AP

TP-LINK Roteador Wireless N 150M
Modelo TL-WR740N / TL-WR740ND

Wireless - Segurança

☐ Desabilitar Segurança

☒ **WEP**

Tipo: Automático

Formato da Chave WEP: ASCII

Chave Selecionada	Chave WEP	Tipo de CHAVE
Chave 1: <input checked="" type="radio"/>	clark	64-bits
Chave 2: <input type="radio"/>		Desabilitado
Chave 3: <input type="radio"/>		Desabilitado
Chave 4: <input type="radio"/>		Desabilitado

Não recomendamos usar a criptografia WEP se o equipamento operar no modo 11n, pelo fato do protocolo WEP não ser suportado pelo padrão 802.11n

☐ **WPA/WPA2**

Versão: Automático

Criptografia: Automático

IP do Servidor Radius:

Porta Radius: 1812 (de 1 a 65535. 0 (zero) representa porta padrão 1812.)

Senha Radius:

Ajuda sobre Wireless - Segurança

Utilize esta página para alterar configurações de segurança de sua rede sem fio. Não é recomendado que a rede fique sem uma senha de acesso definida, pois outros computadores poderão ter acesso não autorizado. Nesta página, você poderá selecionar uma das seguintes opções de segurança:

- Desabilitar Segurança** - A função de segurança do wireless pode ser habilitada ou desabilitada. Se for desabilitada, as estações wireless poderão conectar o Roteador sem criptografia. É fortemente recomendado que você escolha uma das seguintes opções para habilitar a segurança.
- WEP** - Opção de segurança recomendada caso haja na rede sem fio algum dispositivo que não suporte o protocolo WPA, que é mais seguro.
- WPA/WPA2** - Selecione esta opção caso venha a utilizar um servidor de autenticação externo (RADIUS) baseado no protocolo padrão IEEE 802.1x. Esta opção é recomendada apenas para administradores de rede que têm conhecimento aprofundado no assunto.
- WPA-PSK/WPA2-PSK** - Opção ideal para a maioria dos usuários. Os protocolos WPA e WPA2 são os mais seguros no momento, e descomplicados em termos de configuração.

Cada opção de segurança tem suas próprias configurações:

WEP

Tipo - Você pode selecionar um dos seguintes tipos,

- Automático** - Selecione Chave Compartilhado ou Sistema Aberto tipo de autenticação automaticamente

Fonte: Do autor.

Figura 24 - Definição do protocolo WEP versão 128bits e senha no AP

TP-LINK® Roteador Wireless N 150M
Modelo TL-WR740N / TL-WR740ND

Wireless - Segurança

☐ Desabilitar Segurança

☒ **WEP**

Tipo: Automático

Formato da Chave WEP: ASCII

Chave Selecionada

Chave 1: ☒ @3Kx,7(yd6K@o

Chave 2: ☐

Chave 3: ☐

Chave 4: ☐

Chave WEP

Tipo de CHAVE

128-bits

Desabilitado

Desabilitado

Desabilitado

Não recomendamos usar a criptografia WEP se o equipamento operar no modo 11n, pelo fato do protocolo WEP não ser suportado pelo padrão 802.11

☐ **WPA/WPA2**

Versão: Automático

Criptografia: Automático

IP do Servidor Radius:

Porta Radius: 1812 (de 1 a 65535. 0 (zero) representa porta padrão 1812.)

Senha Radius:

Ajuda sobre Wireless - Segurança

Utilize esta página para alterar configurações de segurança de sua rede sem fios. Não é recomendado que a rede fique sem uma senha de acesso definida, pois outros computadores poderão ter acesso não autorizado. Nesta página, você poderá selecionar uma das seguintes opções de segurança:

- Desabilitar Segurança** - A função de segurança do wireless pode ser habilitada ou desabilitada. Se for desabilitada, as estações wireless poderão conectar o Roteador sem criptografia. É fortemente recomendado que você escolha uma das seguintes opções para habilitar a segurança.
- WEP** - Opção de segurança recomendada caso haja na rede sem fios algum dispositivo que não suporte o protocolo WPA, que é mais seguro.
- WPA/WPA2** - Selecione esta opção caso venha a utilizar um servidor de autenticação externo (RADIUS) baseado no protocolo padrão IEEE 802.1x. Esta opção é recomendada apenas para administradores de rede que têm conhecimento aprofundado no assunto.
- WPA-PSK/WPA2-PSK** - Opção ideal para a maioria dos usuários. Os protocolos WPA e WPA2 são os mais seguros no momento, e descomplicados em termos de configuração.

Cada opção de segurança tem suas próprias configurações:

WEP

Tipo - Você pode selecionar um dos seguintes tipos,

- Automático** - Selecione Chave Compartilhado ou Sistema Aberto tipo de autenticação automaticamente

Fonte: Do autor.

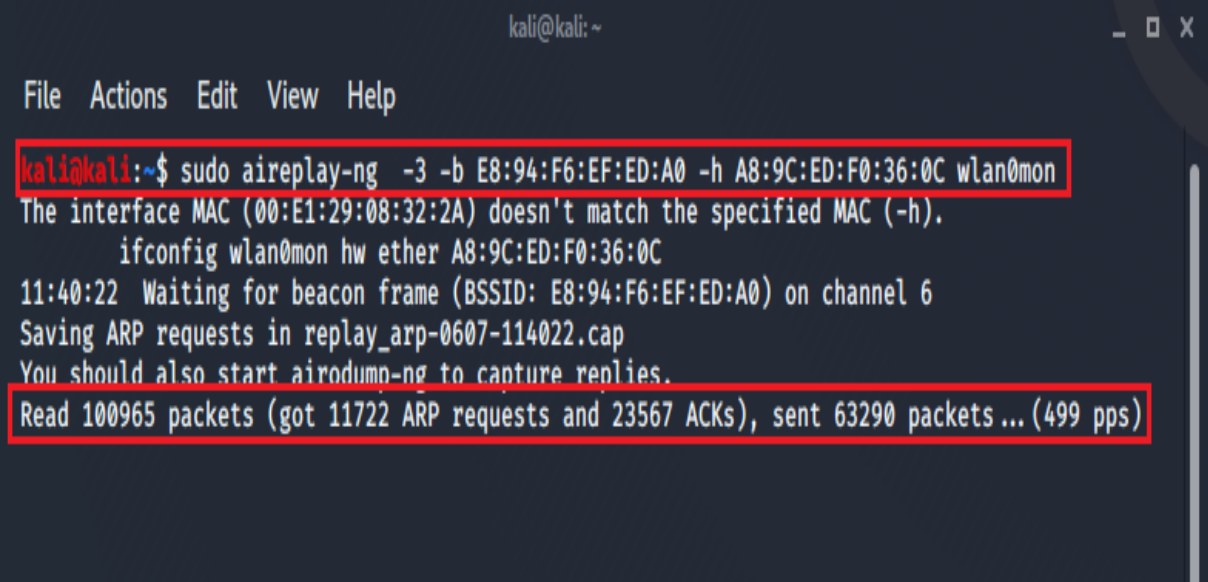
Para que se obtenha sucesso, e consiga quebrar o protocolo WEP e como consequência descobrir a sua senha, se faz necessário capturar um tipo de pacote em especial denominado pacote ARP.

Para que seja garantido à captura desse pacote e a fim de agilizar os testes há a possibilidade de ser feito a utilização do *Aireplay-NG* mais uma ferramenta da suíte *Aircrack-NG*, que como já mencionado, uma de suas funções é a geração de pacotes incluindo os pacotes ARP.

Após seguir as etapas iniciais do subcapítulo 6.5, se faz necessário a criação de um novo terminal, e a execução do seguinte comando: `sudo aireplay-ng -3 --bssid E8:94:F6:EF:ED:A0 -h A8:9C:ED:F0:36:0C wla0mon`. O parâmetro (-3) é a orientação passado dentro do comando, e o parâmetro (-h A8:9C:ED:F0:36:0C) é o endereço BSSID de algum cliente conectado à rede alvo, pois assim a ferramenta *Aireplay-NG* induz esse cliente a gerar mais tráfego do que normalmente geraria, fazendo com que a etapa seja executada com sucesso ao capturar os pacotes ARP.

A imagem 25 demonstra com mais detalhes essa etapa, e comprova a captura dos pacotes ARP.

Figura 25 - Capturando os pacotes ARP



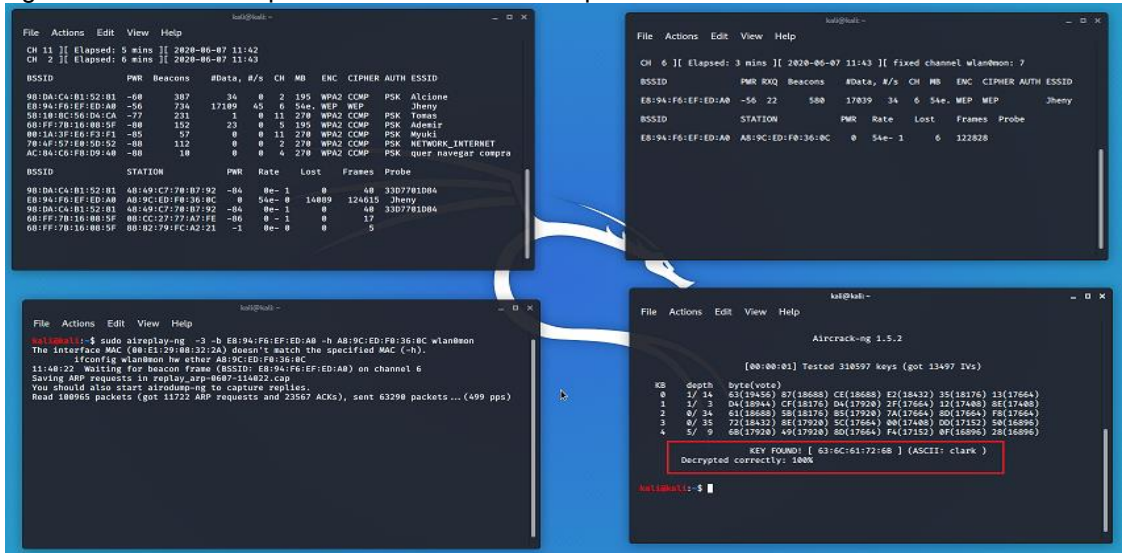
```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo aireplay-ng -3 -b E8:94:F6:EF:ED:A0 -h A8:9C:ED:F0:36:0C wlan0mon  
The interface MAC (00:E1:29:08:32:2A) doesn't match the specified MAC (-h).  
    ifconfig wlan0mon hw ether A8:9C:ED:F0:36:0C  
11:40:22 Waiting for beacon frame (BSSID: E8:94:F6:EF:ED:A0) on channel 6  
Saving ARP requests in replay_arp-0607-114022.cap  
You should also start airodump-ng to capture replies.  
Read 100965 packets (got 11722 ARP requests and 23567 ACKs), sent 63290 packets ... (499 pps)
```

Fonte: Do autor.

Por fim, após capturar os pacotes ARP, já é possível quebrar o protocolo WEP e adquirir sua chave, com a utilização da própria ferramenta *Aircrack-ng*. Se faz então necessário a criação de novo terminal após a execução do comando *sudo aircrack-ng WEP_1.cap*.

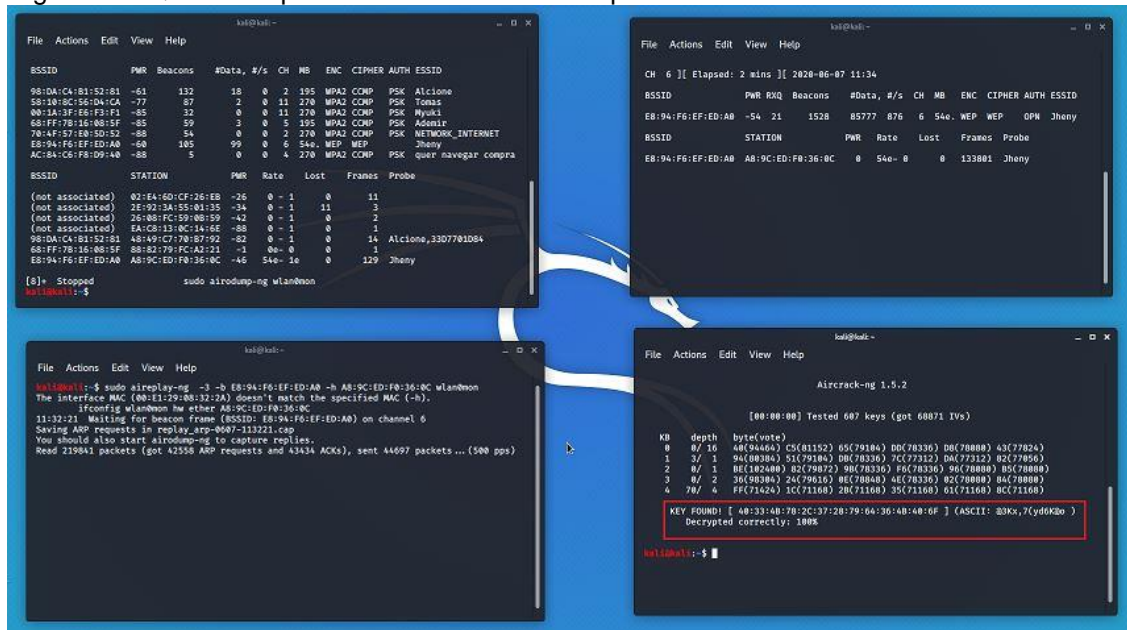
O parâmetro (WEP_1.cap), trata-se do arquivo gerado no passo anterior que é responsável por coletar informações dos pacotes que trafegam pela rede, incluindo os pacotes ARP. Com as imagens 26 e 27, é possível observar que o protocolo WEP foi quebrada e sua chave descoberta em ambas às versões, com sucesso.

Figura 26 - Quebra do protocolo WEP-64bits e captura da senha



Fonte: Do autor

Figura 27 - Quebra do protocolo WEP-128bits e captura da senha



Fonte: Do autor

6.9 QUEBRANDO A CRITOGRAFIA WPA VERSÃO AES E TKIP

Totalizando 30 testes, o tipo de *Pentest* escolhido para a presente protocolo, foi o ataque Dicionário de Senhas com auxílio da captura do *Handshak*.

As técnicas necessárias para quebra do protocolo WPA em ambas as versões AES e TKIP, são um pouco distintas dos protocolos WEP em ambas as versões, isso porque descobrir informações do AP alvo e capturar pacotes não é o suficiente.

Para se obter sucesso na quebra do protocolo WPA em ambas as versões se faz necessário além de saber os dados do AP e capturar os seus pacotes, obter também o *Handshake*, para somente após esse passo utilizar uma *Wordlist*, que como já descrito trata-se de um dicionário de senhas, que com ajuda da ferramenta *Aircrack-NG*, responsável pelo ataque de força bruta com as chaves, realiza testes até que se a chave procurada se encontre neste dicionário a mesma é descoberta pela ferramenta *Aircrack-NG*.

Inicialmente se faz necessário definir o protocolo WPA, sua versão (AES ou TKIP) e senha da mesma no AP, como demonstra a Figura 28 e 29.

Figura 28 - Definição do protocolo WPA-AES e senha no AP

The screenshot shows the 'Configurações Segurança Wireless' (Wireless Security Settings) page of a TP-Link router. The left sidebar lists various configuration options, with 'Wireless' selected. The main content area is titled 'Configurações Segurança Wireless' and includes a warning: 'Para segurança de rede, é altamente recomendável habilitar a segurança wireless e selecionar a criptografia WPA'. There are two main sections: 'Desabilitar Segurança Wireless' (disabled) and 'WPA/WPA2 - Pessoal (Recomendado)' (selected). The 'WPA/WPA2 - Pessoal' section has a red box around its fields: 'Versão' (WPA-PSK), 'Criptografia' (AES), 'Password Wireless' (bheybhiekongmahal), and 'Período de Atualização da Chave de Grupo' (0). Below this is the 'WPA/WPA2 - Empresarial' section, which is currently disabled. The right sidebar contains 'Ajuda com Segurança Wireless' (Wireless Security Help) with instructions on how to choose between different security options.

Fonte: Do autor.

Figura 29 - Definição do protocolo WPA-TKIP e senha no AP

The screenshot shows the TP-Link web interface for a Wireless N 300Mbps router (Model TL-WR849N). The left sidebar contains a navigation menu with options like Status, Configuration, Mode of Operation, Network, Wireless, and Security. The 'Wireless' section is highlighted. The main content area is titled 'Roteador Wireless N 300Mbps' and 'Número do Modelo TL-WR849N'. It displays three security options: 'Desabilitar Segurança Wireless', 'WPA/WPA2 - Pessoal (Recomendado)', and 'WPA/WPA2 - Empresarial'. The 'WPA/WPA2 - Pessoal' option is selected and highlighted with a red box. Under this option, the 'Versão' is set to 'WPA-PSK', 'Criptografia' is set to 'TKIP', and 'Password Wireless' is '9893490614'. The 'Período de Atualização da Chave de Grupo' is set to '0'. To the right, there is a 'Ajuda com Segurança Wireless' section providing additional information about the security options.

Fonte: Do autor.

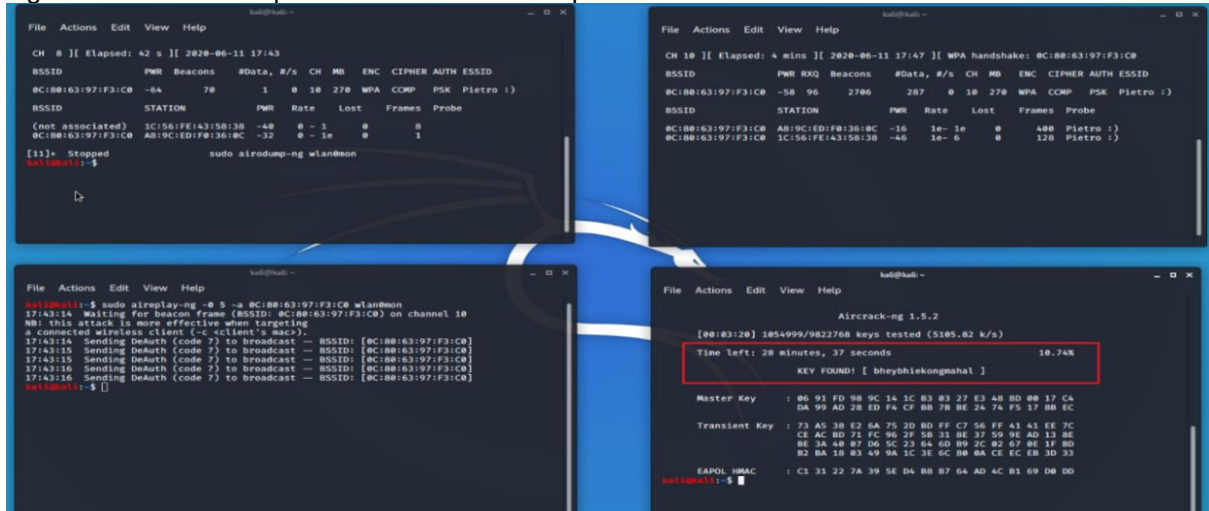
Após seguir as etapas iniciais do subcapítulo 6.5, se faz necessário lançar um ataque de desautentificação ao AP. Inicialmente cria-se um novo terminal, para que seja executado o seguinte comando: `sudo aireplay-ng -0 5 -a 0C:80:63:97:F3:C0`, possibilitando que momentaneamente os clientes conectados ao AP, se desconectem e reconectem automaticamente, pois ao fazer isso o *Handshake* é capturado, permitido assim que a próxima e última parte do teste seja executada.

Tendo capturado o *Handshake*, já é possível efetuar a quebra do protocolo WPA, fazendo o uso da ferramenta *Aircrack-NG*, como auxílio de um dicionário de senhas como o seguinte comando `aircrack-ng WPA_1.cap -w /usr/share/wordlists/rockyou.txt`. O parâmetro (WPA_1.cap) é o nome do arquivo onde foi gravado as informações dos pacotes, e o parâmetro (-w /usr/share/wordlists/rockyou.txt) é o caminho onde se encontra o dicionário de senhas no Kali Linux.

O dicionário de senhas utilizado para o presente trabalho é chamado de *Wordlist Rockyou*. Presente de forma padrão no *Kali Linux* é composto de centenas de senhas reais, que já fizeram a proteção de redes *Wireless*, e que de algum modo foram vazadas na Internet. Realizando uma verificação baseando-se nos códigos e cálculos internos do *Handshake* capturado, e testa com o dicionário, se a senha estiver presente no mesmo ela é capturada.

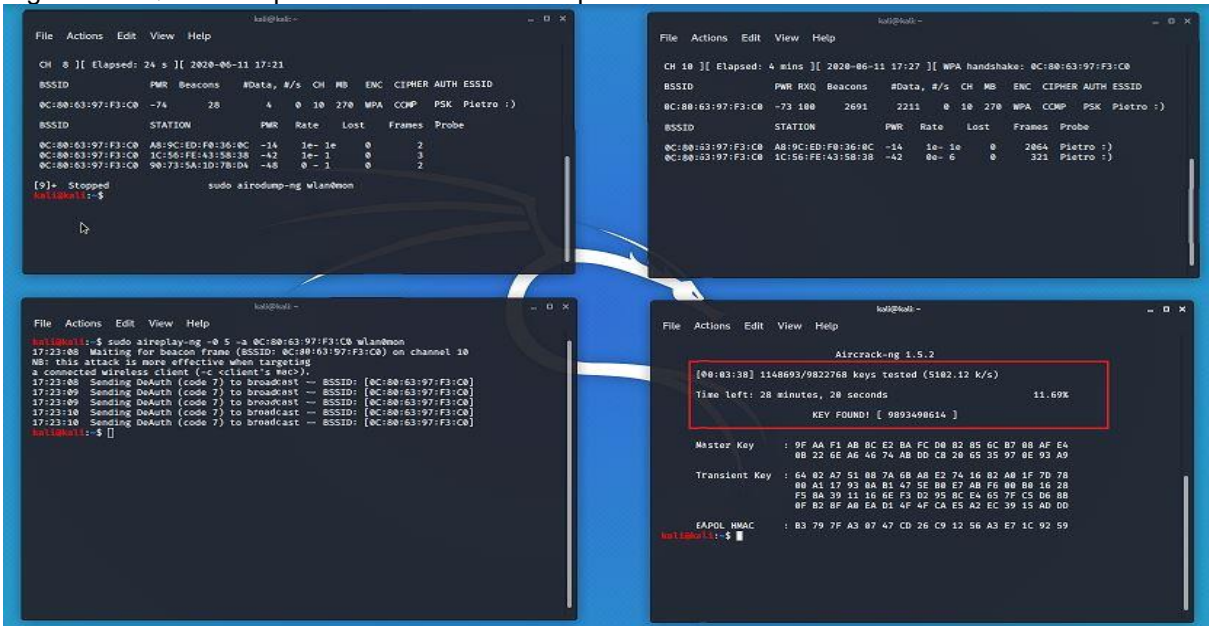
É possível observar nas com as imagens 30 e 31, que o protocolo WPA em ambas as versões foi quebrada e sua chave descoberta, com sucesso.

Figura 30 - Quebra do protocolo WPA-AES e captura da senha



Fonte: Do autor.

Figura 31 - Quebra do protocolo WPA-TKIP e captura da senha



Fonte: Do autor.

6.10 QUEBRANDO A CRITOGRAFIA WPA2 VERSÃO AES E TKIP

Totalizando 45 testes, e seguindo as mesmas etapas do protocolo WPA, o tipo de Pentest escolhido foi o ataque Dicionário de Senhas com auxílio da captura do *Handshak*. Inicialmente se faz necessário definir o protocolo WPA2, sua versão (AES ou TKIP) e senha da mesma no AP, como demonstra a Figura 32 e 33.

Figura 32 - Definição do protocolo WPA2-AES e senha no AP

The screenshot shows the TP-Link web interface for a 'Roteador Wireless N de Alta Potência 300Mbps' (Modelo No. TL-WR841HP). The left sidebar contains navigation links: Status, Configuração rápida, WPS, Rede, Wireless (highlighted), - Configurações do wireless, - Segurança do wireless (highlighted), - Filtro de MAC wireless, - Wireless avançado, - Estatísticas do wireless, Rede visitante, DHCP, Redirecionamento, Segurança, Controle dos pais, Controle de acesso, Roteamento avançado, Controle de largura de banda, Vínculo de IP e MAC, and DNS dinâmico. The main content area is titled 'Segurança do wireless' and has three radio buttons: 'Desativar segurança', 'WPA/WPA2 - Pessoal(Recomendado)', and 'WPA/WPA2 - Empresa'. The 'WPA/WPA2 - Pessoal' option is selected. Below it, the 'Versão' is set to 'WPA2-PSK' and 'Criptografia' is set to 'AES'. The 'Senha do wireless' field contains 'xikdki030407256'. A note states: '(Você pode inserir entre 8 e 63 caracteres ASCII e entre 8 e 64 caracteres hexadecimais.)'. The 'Período de atualização da chave de grupo' is set to '0' segundos, with a note: '(Mantenha o padrão se não tiver certeza, o mínimo é 30 e 0 significa sem atualizações)'. The 'WPA/WPA2 - Empresa' section is also visible, with 'Versão' set to 'Automático', 'Criptografia' set to 'Automático', and fields for 'IP do servidor RADIUS', 'Porta do RADIUS' (1812), and 'Senha do RADIUS'. The 'WEP' section is at the bottom with 'Tipo' set to 'Automático'. On the right, there is a 'Ajuda sobre Segurança do wireless' section with instructions and a list of security options: 'Desativar segurança', 'WPA/WPA2 - Pessoal', 'WPA/WPA2 - Empresa', and 'WEP'. Below this, it says 'Versão - Selecione uma das seguintes versões:' followed by 'Automático', 'WPA-PSK', 'WPA2-PSK', 'WPA-PSK', 'WPA2-PSK', and 'WPA2-PSK'. It also says 'Criptografia - Selecione Automática, TKIP ou AES.' and 'Senha do wireless - Aceita caracteres ASCII ou'.

Fonte: Do autor.

Figura 33 - Definição do protocolo WPA2-TKIP e senha no AP

This screenshot is similar to the previous one, but the 'Criptografia' is set to 'TKIP'. The 'Senha do wireless' field now contains 'marvin24'. A red warning box appears below the password field, stating: 'Não é recomendável utilizar a criptografia TKIP se este dispositivo funciona no modo 802.11n uma vez que eles não são compatíveis.' The rest of the interface, including the sidebar and the right-hand help section, remains the same as in Figure 32.

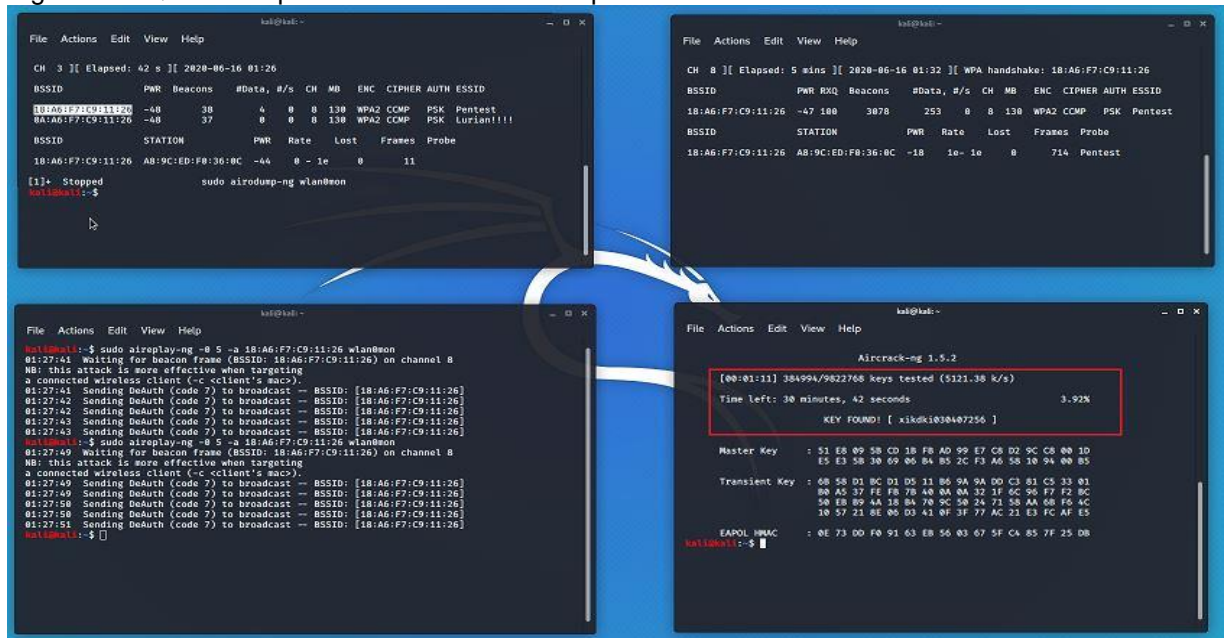
Fonte: Do autor.

Após seguir as etapas iniciais do subcapítulo 6.5, para que se obtenha sucesso no presente teste é necessário lançar um ataque de desautentificação ao AP. Cria-se um novo terminal, para a execução do comando em seguida: `sudo aireplay-ng -0 5 -a 0C:80:63:97:F3:C0`, possibilitando que momentaneamente os clientes conectados ao AP, se desconectem e reconectem automaticamente, ao realizar esse ataque o *Handshake* é capturado, permitido assim que a próxima e última etapa do teste seja executada.

Após capturar o *Handshake*, já é possível efetuar a quebra do protocolo WPA em ambas as versões, fazendo o uso da ferramenta *Aircrack-NG*, como auxílio de um dicionário de senhas.

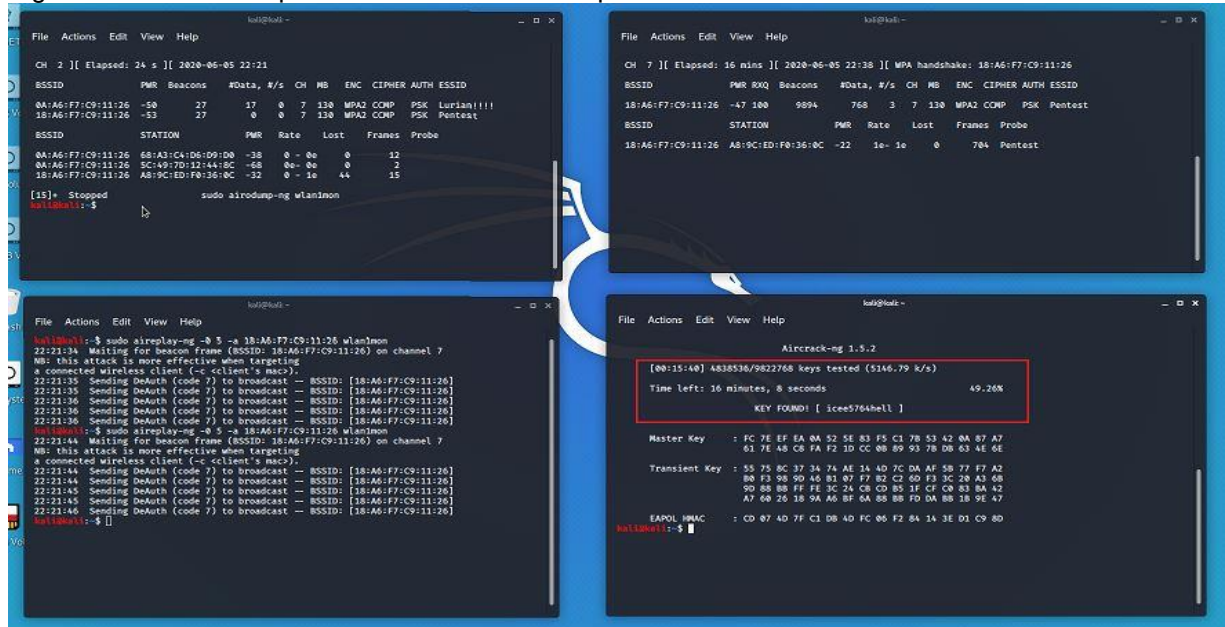
Com as imagens 34 e 35 é possível observar que o protocolo WEP foi quebrado e sua chave descoberta em ambas às versões, com sucesso.

Figura 34 - Quebra do protocolo WPA2-AES e captura da senha



Fonte: Do autor.

Figura 35 - Quebra do protocolo WPA2-TKIP e captura da senha



Fonte: Do autor.

6.11 QUEBRANDO A CRITOGRAFIA WPA3

Como já abordado em junho de 2018, a *Wi-Fi Alliance* anunciou o WPA3 como a próxima geração de protocolo *Wireless*. Este novo mecanismo tem como objetivo, oferecer mais segurança aos usuários de redes *Wireless* ao acrescentar mecanismos de proteção ao seu antecessor WPA2. Estes mecanismos incluem a dificuldade acentuada contra ataques de dicionário, resistência no ataque de desautentificação dentre outros. Até o presente momento não se sabe muito mais do que se faz presente em artigos científicos e das poucas informações que se fazem presente no site oficial da *Wi-Fi Alliance*.

Todavia apesar da indisponibilidade dos dispositivos com o protocolo WPA3 no mercado, em abril de 2019, os pesquisadores descobriram um conjunto de vulnerabilidades, na mesma. Com base na especificação do protocolo WPA3 disponível e uma colaboração com um fornecedor de dispositivos, foi demonstrado um conjunto de ataques, variando desde a negação de serviço até a quebra da senha da rede *Wireless* com a utilização do protocolo WPA3. (LOUNIS; ZULKERNINE, 2019, tradução nossa).

Infelizmente como já mencionado, o protocolo WPA3 ainda não se encontra no mercado principalmente o Brasileiro, outro empecilho foi dada a atual condição mundial, com a pandemia do Covid-19 atenuada com a alta do dólar, que impossibilitou a importação de um AP com o protocolo WPA3.

Por esses motivos se tornou impossível realizar os testes de *Pentest* como foi realizado com os demais protocolos, afim de dar continuidade a esse trabalho optou-se então por realizar o levantamento de dados dos *Pentest*, baseando-se nos artigos científicos de pesquisadores ao redor do mundo, que já tiveram contato com a mencionado protocolo, e realizaram os mesmos testes de *Pentest* abordados nesse trabalho.

6.11.1 Ataque de Desautentificação

Para realizar o ataque são enviados pacotes de desautenticação para um ou mais clientes, falsificando o endereço MAC do AP para desautenticar o cliente e cortar a conexão com o AP.

Quando um cliente recebe um pacote de desautenticação ou dissociação não criptografada do AP que já está em sessão, o mesmo envia uma solicitação de consulta *Security Association* (SA) criptografada para o AP, e aguarda uma resposta dentro do tempo de resposta.

O AP real é capaz de responder com uma resposta de consulta SA protegida e ignorar qualquer pacote de desautenticação. Portanto, a realização de um ataque de desautenticação com o protocolo WPA3 é inviável. (KOHLIOS; HAYAJNEH, 2018, tradução nossa)

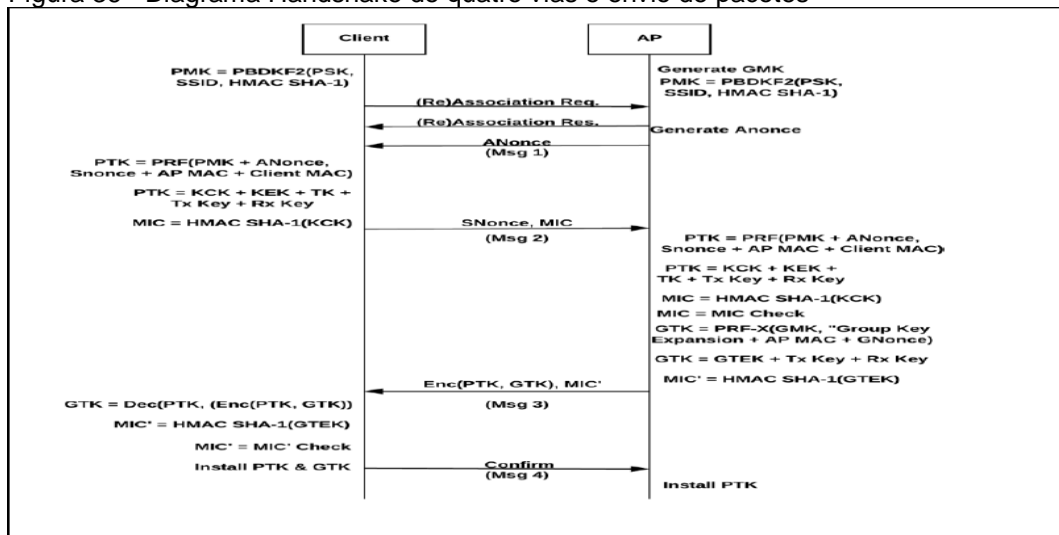
6.11.2 Ataque Krack

Conforme já mencionado o ataque *KRACK* aproveita a vulnerabilidade do reenvio pacotes no *Handshake* de quatro vias para obter capacidade de descriptografar o tráfego de um cliente sem precisar capturar o *Handshake* e ter que conhecer a chave.

Nesse tipo de ataque, o invasor engana a vítima para reinstalar uma chave já em uso. E assim faz com que, alguns parâmetros associados à protocolo que asseguram o controle da comunicação são resetados.

Tais falhas não permitem ao invasor recuperar a senha *Wireless*, mas sim descriptografar os dados sem mesmo saber a senha. A Figura 36 demonstra um diagrama detalhado do Handshake de quatro vias e do envio de pacotes.

Figura 36 - Diagrama Handshake de quatro vias e envio de pacotes



Fonte: Adaptado de Kohlios e Hayajneh (2018).

A fim de impossibilitar esse ataque, *Patches* foram criados a fim de não permitir essa retransmissão desses pacotes. Com patches de segurança e configurações atualizadas, um roteador WPA3 pode ser configurado para não permitir a retransmissão dos pacotes, que é parte integrante do ataque.

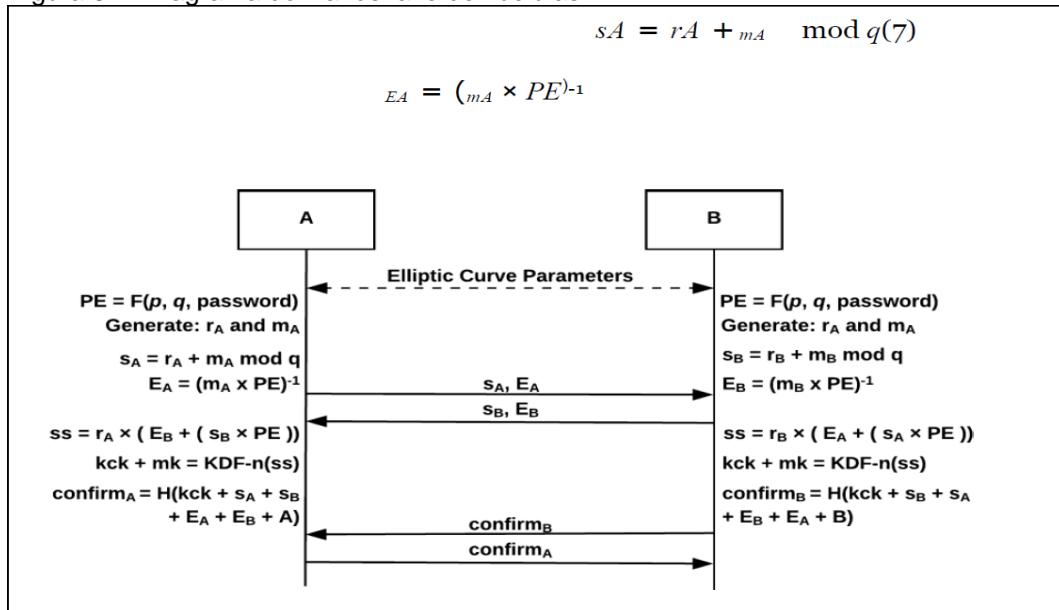
Portanto, o ataque KRACK é inviável. (VANHOEF; PIESENS, 2017, tradução nossa).

6.11.3 Ataques de Dicionário com captura do Handshake

No protocolo WPA2, um invasor é capaz de capturar os dois *nonces* aleatórios gerados *Handshake* de quatro vias, e obtê-los em formato de texto simples para usá-los, em conjunto com a senha, e assim derivar o PTK e descriptografar o tráfego. O protocolo WPA3 opera com o protocolo SAE, que utiliza o *Handshake* de

libélula e o de quatro vias, sendo assim o invasor não seria capaz de capturar informações dos dois *Handshake* e derivar um PTK para descriptografar o tráfego. O mesmo tentará capturar mensagens do *Handshake* de libélula, obtendo apenas os seguintes dados EA, EB, sA e sB, conforme a Figura 37.

Figura 37 - Diagrama do Handshake de libélulas



Fonte: Adaptado de Kohlios e Hayajneh (2018).

Para obter o PMK utilizado no *Handshake* de quatro vias, o invasor deve calcular os segredos compartilhados, definidos nas formulas (3), (4) e (5):

$$ss = rA \times ((mB \times PE) - 1 + ((rB + mB) \times PE)) \quad (3)$$

$$ss = rA - ((mB \times PE) + (mB \times PE)) \quad (4)$$

$$ss = rA \times rB \times PE = rB \times rA \times PE \quad (5)$$

Para assim obter conhecimento de rA e rB para realização do cálculo, simultaneamente com o elemento de senha PE. O PE é capaz de ser derivado usando a senha conhecida como semente em uma função conhecida, dados os parâmetros da curva elípticos capturados p e q .

Entretanto é computacionalmente impossível obter mA dado EA e PE. Assim, o invasor não seria capaz de derivar um PMK e PTK para comparar com um MIC capturado e descobrir a senha correta existente no dicionário de senhas.

Portanto, a decodificação da senha com auxílio do *Handshake* e do dicionário de senhas é inviável no protocolo WPA3. (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

Porém inicialmente com a chegada gradativa do WPA3, um AP aceita conexões usando WPA3-SAE e WPA2 com a mesma senha, mais conhecido como *Downgrades*. Isso fornece compatibilidade para usuários que possuam dispositivos mais antigos, e que por sua vez ainda não suportam o protocolo WPA3, somete a WPA2.

Sabendo disso um invasor pode se beneficiar, pois como já mencionado o protocolo WPA2, é suscetível a ataques de que capturam o seu *Handshake*, e nesse modo de retrocompatibilidade o protocolo WPA3 não consegue impedir, que o adversário capture dados suficientes de um *Handshake* para realizar um ataque de dicionário e com isso descobrir a senha.

Foi descoberto que dispositivos como Samsung Galaxy S10 e o iNet Wireless *Daemon* são afetados por *Downgrades*. Mesmo quando esses dispositivos se conectam a uma rede WPA3 pura, um adversário ainda pode forçá-los a usar o WPA2. Pois assim é viável que um adversário recupere a senha da rede usando ataques de força bruta ou de dicionário (VANHOEF; RONEN, 2019, tradução nossa).

6.11.4 Ataque Evil Twin

Com relação ao ataque *Evil Twin*, nem um protocolo é capaz de realmente proteger usuário, pois há uma dificuldade de conseguir impedir a geração de um AP falso, e com o protocolo WPA3 não é diferente.

O modo de estrutura do ataque é o mesmo citado com os outros protocolos, porém ao realizar o ataque desautenticação para o AP alvo, a fim de suspender a

conexão do cliente com o AP genuíno, o protocolo WPA3 não permitirá que o mesmo aconteça, fazendo com que o invasor não obtenha sucesso no ataque.

Porem uma alternativa seria o induzir a vítima, para que a mesma se conecte diretamente ao AP falso, oferecendo um sinal mais forte. Seguindo os mesmos passos, porém sem necessitar realizar o ataque de desautenticação realizando assim uma conexão confiável com o AP falso possibilitando ao invasor descriptografar todo o tráfego usando o PTK além de ter a possibilidade de levar a vítima a inserir a senha correta do AP verdadeiro ao simular a necessidade de inserção da mesma no ato da conexão com o AP falso. Uma vez fora da rede, o protocolo WPA3 já não protege os dados do cliente. Portanto, é possível realizar um ataque de *Evil Twin*. (KOHLIOS; HAYAJNEH, 2018, tradução nossa)

O protocolo WPA3 conta ainda com outras vulnerabilidades, porém não foram detalhados no presente trabalho, pois foi dada preferência por abordar as mesmas que também se fazem presente nos outros protocolos já abordadas, principalmente a WPA2.

Para Lounis e Zulkernine (2019, tradução nossa), apesar protocolo do WPA3 ainda estar sendo implementada pelos fabricantes de dispositivo Wireless, foi demonstrado que a mesma possui vulnerabilidades que podem vir a afetar a segurança de toda a rede, sendo considerado algo grave, pois o protocolo WPA3 deveria substituir o protocolo WPA2 por uma segurança e instabilidade mais elevada.

Na visão de Kohlios e Hayajneh (2018, tradução nossa), o novo padrão do protocolo WPA3 corrige muitos dos problemas presentes no protocolo WPA2, incluindo a desautenticação, os ataques de dicionário off-line e a vulnerabilidade *KRACK*, porém não resolve algumas das principais vulnerabilidades das redes *Wireless*. No entanto, podem ser empregadas defesas e práticas seguras para auxiliar a manter a segurança mesmo diante dessas ameaças.

Já na opinião de Vanhoef e Ronen (2019, tradução nossa), as principais fraquezas do protocolo WPA3 são ataques de *Downgrade* e possíveis ataques de tempo contra dispositivos com recursos limitados. Os ataques de desvio de autenticação contra o EAP-pwd implementados no *Dragonslayer* que também demonstram problemas críticos na segurança. Porem mesmo que não seja

apresentada uma variante melhor do protocolo WPA3 é indicado mudar para a mesma assim que estiver disponível, pois é esperado que atualizações futuras partido dos fornecedores de dispositivo Wireless, diminuam a maioria dos problemas encontrados o que significa que a WPA3 ainda será uma melhor opção em relação a WPA2. Para realização de futuros trabalhos sugere-se reavaliar o protocolo WPA3, a fim de verificar se houve atualizações, que gerem melhoria na mesma a fim de sanar as fraquezas apontadas nesse trabalho.

6.12 RESULTADOS OBTIDOS E DISCUSSÃO

Com os testes de *Pentest* realizados com os protocolos WEP, WPA, WPA2 observou-se os seguintes resultados. Foi concluída que o protocolo WEP em suas versões 64 e 128 bits, é a mais fraca criptografia, pois mesmo na versão 128 bits sendo possível fazer o uso de uma senha mais complexa do que na versão 64 bits, a protocolo é quebrada e a senha descoberta sem maiores dificuldades.

Já com os protocolos WPA e WPA2, mesmo sendo mais robustas e necessitem da descoberta de mais dados juntamente com um ataque mais elaborado, também se mostraram vulneráveis aos ataques ministrados, mesmo quando utilizado uma senha maior com caracteres maiúsculos, minúsculos, especiais e números juntos as mesmas eram quebradas e suas senhas descobertas.

Com relação ao protocolo WPA3, baseando-se nos artigos científicos e os documentos para o estudo realizado, observa-se melhorias com relação a sua antecessora o protocolo WPA2, porém os mesmo herdou algumas de suas vulnerabilidades, onde pode-se observar que um ataque mais elaborado ainda se faz possível aproveitar-se dessas vulnerabilidades para realizar a quebra do protocolo e descobrir a senha do mesmo.

Levando em consideração todas as informações presentes neste trabalho é possível observar, que uma configuração correta do AP se faz necessária, com intuito de auxiliar os protocolos no quesito segurança como, por exemplo, a função WPS, que como mencionado com os resultados obtidos se fez resistente aos testes de *Pentest* ministrados, porem como a tecnologia está em constante desenvolvimento

e com ela os tipos de ataques evoluem e também novos são criados, e levando em consideração que mesma não se faz necessária para a utilização de uma rede *Wireless*, poderia ser desativada sem problemas.

A utilização dos mais novos protocolos sendo ela o WPA2 ou WPA3, com uma senha robusta e bem elaborada, pois mesmo que não garanta segurança total cria um obstáculo que dificulta ao máximo a invasão do AP. E por último realizar a troca periódica da senha pode ser de grande auxílio e garantir a segurança.

O presente trabalho obteve resultados similares com o de seus trabalhos correlatos, e chegando a alguns casos a obter os mesmos, com relação aos testes de Pentest.

Com o trabalho *Segurança em redes Wireless domésticas: Um Estudo de Caso* o mesmo apresentou basicamente os mesmo testes de *Pentest* abordados no presente trabalho. Os resultados obtidos quando não os mesmos foram próximos, somente modificando os cenários.

Já com o trabalho *Análise e Proposta de Melhoria na Estrutura de Redes Sem Fio em Escolas Públicas na Microrregião de Araranguá*, demonstrou a importância da configuração correta dos AP's em escolas, tendo em vista a posição correta dos AP's e o local onde foram estrategicamente colocados, a fim de garantir cobertura total do âmbito escolar.

Também foram realizadas todas as medidas necessárias para garantir a segurança dos usuários na utilização da rede *Wireless*, demonstrando assim como o presente trabalho o quão importante é realizar a configuração correta do AP.

Os TCC's *Análise de Padrões de Segurança em Redes Sem Fio IEEE 802.11* e *Estudos de Caso de Segurança em Redes Sem Fio Utilizando Ferramentas Para Monitoramento e Detecção de Ataques* os resultados com o presente trabalho foram muito semelhantes, somente com algumas exceções voltada a algumas particularidades dos temas de cada um.

O trabalho correlato *Um Modelo Abrangente de Fluxo de Ataque e Análise de Segurança para Wi-Fi e WPA3*, onde o mesmo apontou as principais atualizações do protocolo WPA3 e realizou os testes de *Pentest* com o mesmo.

7 CONCLUSÃO

O presente trabalho por meio dos testes de *Pentest* demonstrou a falta de segurança nos protocolos WEP, WPA, e WPA2, conforme bibliografia consultada, e foi possível demonstrar. Mas o novo protocolo WPA3, não foi realizado os testes de *Pentest*. Desta forma, os resultados e conclusões foram obtidos com base nas pesquisas bibliográficas.

Com o avanço da tecnologia os métodos de invasão aos protocolos se tornam cada vez mais robustos, tendo em vista isso a indústria criou o protocolo WPA3. Conforme os resultados e discussões, o mesmo não supriu as necessidades de segurança necessárias nos dias atuais, trazendo consigo vulnerabilidades que inclusive foram herdadas de seu antecessor o protocolo WPA2, como por exemplo a vulnerabilidade de retrocompatibilidade, que explora a compatibilidade do protocolo WPA3 com seu antecessor o WPA2, tendo em vista que no primeiro momento os dispositivos não terão total compatibilidade com o novo protocolo WPA3, assim que o mesmo se fizer amplamente presente nos AP's.

Sendo assim, é recomendado a configuração correta dos AP's, como por exemplo utilizar sempre o protocolo de segurança mais atual, sendo eles o WPA2 ou WPA3, utilizar uma senha robusta composta por números, letras e caracteres especiais e sempre que possível substituí-la por outra com regularidade como forma de elevar a segurança e assim auxiliar o protocolo escolhido, pois se sabe que em alguns casos a má configuração do mesmo acaba acarretando mais problemas à segurança que as próprias falhas dos protocolos e criptografias.

Observa-se as boas práticas de utilização, e estas devem ser amplamente empregadas por todos os usuários, de forma a não expor os dados, com algum ataque relacionado a vírus e malwares.

Com o protocolo WPA3 espera-se que o mesmo receba atualizações para que se torne ainda mais robusto, pois assim de fato possa vir a substituir a sua antecessora com o devido propósito a que lhe foi atribuído em sua criação.

Recomenda-se para trabalhos futuros, sugerindo para que tendo em posse de um AP com o protocolo WPA3, reavaliar a protocolo, a fim de verificar se houve

atualizações que gerem melhoria do mesmo, e assim sanar os problemas apontados nesse trabalho.

REFERÊNCIAS

BEDNARCZYK, Mariusz; PIOTROWSKI, Zbigniew. **"Will WPA3 really provide Wi-Fi security at a higher level?"**, Proc. SPIE 11055, XII Conference on Reconnaissance and Electronic Warfare Systems, 1105514 (27 de Março de 2019); doi: 10.1117/12.2525020; <<https://doi.org/10.1117/12.2525020>>. Acesso em 20/05/2019.

BELLARDO, John; SAVAGE, Stefan. **802.11 Ataques de negação de serviço: vulnerabilidades reais e soluções práticas**. 2003. 8 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade da Califórnia em San Diego, Califórnia, 2003. Disponível em: <https://www.usenix.org/legacy/event/sec03/tech/full_papers/bellardo/bellardo_html/>. Acesso em: 21/05/2019.

BORISOV, Nikita. Goldberg, Ian. Wagner, David. (2001). **Intercepting Mobile Communications: The Insecurity of 802.11**. **Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM**. 10.1145/381677.381695. Disponível em: <https://www.researchgate.net/publication/2395032_Intercepting_Mobile_Communications_The_Insecurity_of_80211>. Acesso em: 14/04/2019.

BRASIL. Casa Civil. **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012**. 2012. 2 f. Tese (Doutorado) - Curso de Assuntos Jurídicos, Presidência da República, Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10/06/2019.

CAÇADOR, Daniel Maximino. **Segurança e Mobilidade em Redes IEEE 802.11: Modelo de suporte à decisão na escolha de arquiteturas e tecnologias de redes sem fios**. 2014. 175 f. Dissertação (Mestrado) - Curso de Engenharia, Universidade Católica Portuguesa, Portugal, 2014. Disponível em: <<https://repositorio.ucp.pt/bitstream/10400.14/17480/1/Disserta%C3%A7%C3%A3o%20Mestrado%20SSI%20Daniel%20Cacador%20Final%20-%20Revista.pdf>>. Acesso em: 14/04/2019.

CARLESSI, Lucas da Silva. **Estudos De Caso De Segurança Em Redes Sem Fio Utilizando Ferramentas Para Monitoramento E Detecção De Ataques**. 2011. 97 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense-unesc, Criciúma, 2011. Disponível em: <<http://tcc.kironunesc.net.br/arquivos/trabalhos/279.pdf>>. Acesso em: 12/05/2019.

CERT.br. **O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. 2018. Disponível em: <<https://www.cert.br/>>. Acesso em: 10/06/2019.

CIFUENTES, Nayaret; GATICA, Gustavo; LINFATI, Rodrigo. **Un modelo de programación lineal para el problema de máquinas paralelas no relacionadas en el área de secado de un aserradero en Chile**. Revista Facultad de Ingeniería, [s.l.], v. 26, n. 46, p. 71-78, 5 set. 2017. Universidad Pedagógica y Tecnológica de Colombia. <http://dx.doi.org/10.19053/01211129.v26.n46.2017.7309>. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=6359518>. Acesso em: 17 jun. 2020.

CODEVANT. **Pentest – Passo a Passo e Métodos**. 2018. Disponível em: <https://www.codevant.com/appsec/Pentest/>. Acesso em: 18/10/2018.

CORRÊA, Underléa; AL, Et. **Redes Locais Sem Fio: Conceito e Aplicações**. 2006. 41 f. Monografia (Especialização) - Curso de Engenharia Elétrica, Departamento de Automação e Sistemas, Universidade Federal de Santa Catarina, Florianópolis, 2006. Disponível em: https://s3.amazonaws.com/academia.edu.documents/4934221/minicurso_redeslocais.pdf?response-content-disposition=inline%3B%20filename%3DRedes_Locais_Sem_Fio_Conceito_e_Aplicaco.pdf. Acesso em: 25/05/2019.

COSTA, Flávio Wesler de. **Análise de Padrões de Segurança em Redes Sem Fio IEEE 802.11**. 2009. 106 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense-unesc, Criciúma, 2009. Disponível em: <http://tcc.kironunesc.net.br/?id=604&procura=&onde=0&order=0&area=&pchave=&inicial=-1&final=-1&orientador=&coorientador=>>. Acesso em: 10/04/2019.

COUTO, Lucas Oliveira do. Modelo de guia de boas práticas de configuração e uso para a segurança da operação de redes WPA-PSK. Orientador: Prof. Dr. Tiago Alves da Fonseca. 2018. 123 f. Trabalho de Conclusão de Curso (Bacharel) - Universidade de Brasília, [S. l.], 2018. Disponível em: https://www.bdm.unb.br/bitstream/10483/21584/1/2018_LucasOliveiraDoCouto_tcc.pdf. Acesso em: 25 jun. 2020.

CYBERPUNK. **Wireless security protocols**. 2018. Disponível em: <https://www.cyberpunk.rs/wireless-security-protocols-wep-wpa-wpa2-and-wpa3>. Acesso em: 10/04/2019.

FERREIRA, Rui A. C.. A Probability Problem Arising from the Security of the Temporal Key Hash of WPA. **Wireless Personal Communications**, [s.l.], v. 70, n. 4, p.1235-1241, 5 jul. 2012. Springer Nature. Disponível em: <https://link.springer.com/article/10.1007%2Fs11277-012-0744-x>. Acesso em: 18/04/2019.

FLUHRER, Scott; MANTIN, Itsik; SHAMIR, Adi. **Weaknesses in the Key Scheduling Algorithm of RC4**. Springer-verlag Berlin Heidelberg, Usa, v. 1, n. 1, p.1-24, 2001. Disponível em: https://link.springer.com/content/pdf/10.1007%2F3-540-45537-X_1.pdf. Acesso em: 26/06/2019.

G1. **Mundo tem 3,2 bilhões de pessoas conectadas à internet, diz UIT.**

Disponível em: <<http://g1.globo.com/tecnologia/noticia/2015/05/mundo-tem-32-bilhoes-de-pessoas-conectadas-internet-diz-uit.html>>. Acesso em: 27 set. 2018.

GARCIA, Luiz Guilherme Uzeda. **Redes 802.11 (Camada de Enlace): Redes locais sem fio que atendem ao padrão IEEE 802.11. 2001.** Disponível em: <https://www.gta.ufrj.br/grad/01_2/802-mac/index.html>. Acesso em: 11/04/2019.

GOYAL, Vipul et al. **A new protocol to counter online dictionary attacks. Computers & Security**, [s.l.], v. 25, n. 2, p.114-120, mar. 2006. Elsevier BV. <http://dx.doi.org/10.1016/j.cose.2005.09.003>. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0167404805001537>>. Acesso em: 30/05/2019.

HADIDSAMA. **Trusted digital marketing service.** 2010. Disponível em: <https://hadidsama.com/services/jaringan-komputer/>. Acesso em: 18/10/2018

HWANG, Hyunuk et al. A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP. **2008 International Conference On Information Science And Security (iciss 2008)**, [s.l.], p.164-170, jan. 2008. IEEE. <http://dx.doi.org/10.1109/iciss.2008.10>. Disponível em: <<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4438228&isnumber=4438195>>. Acesso em: 30/05/2019.

KOHLIOS, Christopher; HAYAJNEH, Thaier. **A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics**, [s.l.], v. 7, n. 11, p.284-312, 30 out. 2018. MDPI AG. <http://dx.doi.org/10.3390/electronics7110284>. Acesso em: 15/05/2019.

KOZIOL, Michael. **Wi-Fi Gets More Secure: Everything You Need to Know About WPA3:** WPA3, Enhanced Open, Easy Connect: The Wi-Fi Alliance's trio of new protocols explained. 2018. Disponível em: <<https://spectrum.ieee.org/tech-talk/telecom/security/everything-you-need-to-know-about-wpa3>>. Acesso em: 18/04/2019.

LEHEMBRE, Guillaume. **Seguridad Wi-Fi – WEP, WPA y WPA2. Haking**, Espanha, v. 067, n. 01, p.12-26, jan. 2006. Disponível em: <http://www.zero13wireless.net/wireless/seguridad/01_2006_wpa_ES.pdf>. Acesso em: 19/04/2019.

LEPESQUEUR, Alexandre Mendes Alvim; OLIVEIRA, Italo Diego Rodrigues. **Pentest, Análise e Mitigação de Vulnerabilidades.** 2012. 89 f. TCC (Graduação) - Curso de Faculdade de Tecnologia, Engenharia Elétrica,

Universidade de Brasília, Brasília, 2012. Disponível em: <http://bdm.unb.br/bitstream/10483/13510/1/2012_AlexandreMendesAlvimLepesqueur_ItaloDiegoRodriguesOliveira.pdf>. Acesso em: 15/06/2019.

LESSA, Felipe Almeida. **O protocolo WEP: Sigilo contra Acidentes**. 2009. 21 f. TCC (Graduação) - Curso de Sistemas de Informação, Universidade de Brasília, Brasília, 2009. Disponível em: <<https://cic.unb.br/~pedro/trabs/lessa.pdf>>. Acesso em: 21/04/2019.

LOUNIS, Karim; ZULKERNINE, Zulkernine. **Bad-Token: Denial of Service Attacks on WPA3**. [S. l.], p. 1-8, 15 dez. 2019. DOI <https://doi.org/10.1145/3357613.3357629>. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3357613.3357629>. Acesso em: 30 jun. 2020.

MALBURG, Maria Moura. **Trabalho Final de Redes I**. 2004. Disponível em: <https://www.gta.ufrj.br/grad/04_2/Modulacao/>. Acesso em: 18/05/2019.

MILLS, Matt. **O que é o WPS dos roteadores, como funciona e por que você deve desativá-lo**. 2019. Disponível em: <https://itigic.com/pt/what-is-the-wps-of-the-routers-how-it-works/>. Acesso em: 25 jun. 2020.

MORENO, Daniel. **Introdução ao Pentest**. São Paulo: Novatec, 2015. 296 p
MORETTI, Cleber; BELLEZI, Marcos Augusto. **Segurança em Redes Sem Fio 802.11. Tecnologias, Infraestrutura e Software, T.i.s**. São Carlos, v. 1, n. 3, p.24-33, abr. 2014. Disponível em: <<http://revistatis.dc.ufscar.br/index.php/revista/article/viewFile/73/67>>. Acesso em: 20/05/2019.

_____, Daniel. **Pentest em redes sem fio**. São Paulo: Novatec, 2016. 320 p.
BARBOSA, Gracieiny A. et al. **Estudo de Caso: Vulnerabilidades em Rede Wireless**. Revista Gestão em Foco, São Paulo, v. 9, n. 9, p.1-20, mar. 2017. Disponível em: <http://www.unifia.edu.br/revista_eletronica/revistas/gestao_foco/artigos/ano2017/057_estudo10.pdf>. Acesso em: 20/05/2019.

NORTON. **Norton Cyber Security Insights Report Global Results**. Symantec, U. S, 2018. Disponível em: <<https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf>>. Acesso em: 21/04/2019.

OLIVEIRA, Lucas Vinícius de; BEM, Ricardo Orige de. **Análise e proposta de melhoria na estrutura de redes sem fio em escolas públicas na microrregião de araranguá.** 2017. 82 f. TCC (Graduação) - Curso de Tecnologias da Informação e Comunicação, Universidade Federal de Santa Catarina-campus Araranguá, Araranguá, 2017. Disponível em: <<https://repositorio.ufsc.br/bitstream/handle/123456789/178597/TCC%20POSTAR%20AGORA.pdf?sequence=1&isAllowed=y>>. Acesso em: 20/05/2019.

ROCHA, Adrielle T. Q.; COSTA, Bruno N. L. GIUZEPE, Kessius V. L. MARTINS, Henrique P. **Pentest para Quebra de Protocolo Wireless.** 2016. 20 f. Tese (Doutorado) - Curso de Redes de Computadores, Faculdade de Tecnologia de Bauru (fatec-bauru), Bauru, 2016. Disponível em: <<http://www.fatecbauru.edu.br/ojs/index.php/CET/article/viewFile/203/174>>. Acesso em: 10/06/2019.

SANATINIA, Amirali et al. Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study. *Ieee Conference On Communications And Network Security (cns)*, National Harbor, Md, p. 430-437, set. 2013. Disponível em: <https://ieeexplore.ieee.org/document/6682757>. Acesso em: 25 jun. 2020.

SOUZA, Fabrício R. A.; SILVA, Cristiano Maciel da; GUIMARÃES, Cayley. **Segurança em Redes Wireless.** 2013. 12 f. Tese (Doutorado) - Curso de Ciência da Computação, Uni-bh, Belo Horizonte, 2013. Disponível em: <<http://revistas.unibh.br/index.php/dcet/article/download/236/128>>. Acesso em: 18/05/2019.

STANGARLIN, Douglas Pegoraro; PRIESNTZ, Walter Filho. **Análise de Desempenho de Redes Sem Fio com Diferentes Protocolos de Protocolo.** 2012. 4 f. Monografia (Especialização) - Curso de Redes, Universidade Federal de Santa Maria, Santa Maria, 2012. Disponível em: <https://www.researchgate.net/publication/255622824_Analise_de_Desempenho_de_Redese_Sem_Fio_com_Diferentes_Protocolos_de_Protocolo>. Acesso em: 22/05/2019.

SWATI, Sukhija; SHILPI, Gupta, “**Wireless Network Security Protocols a Comparative Study**”, *International Journal of Emerging Technology and Advanced Engineering*, 2(1), 2012.

TANENBAUM, Andrew S.. **Redes de Computadores.** 4. ed. Rio de Janeiro: Campus, 2003.968 p.

VANHOEF, Mathy; PIESENS, Frank. **Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Ccs'17**, Dalas, Tx, Usa, n. 1, p.1-20, 03 nov. 2017. Disponível em: <<https://papers.mathyvanhoef.com/ccs2017.pdf>>. Acesso em: 30/05/2019.

VANHOEF, Mathy; PIESENS, Frank. **Practical Verification of WPA-TKIP Vulnerabilities**. 2016. 9 f. Dissertação (Mestrado). Curso de Ciências da Computação, Estados Unidos. Disponível em: <<http://papers.mathyvanhoef.com/asiaccs2013.pdf>>. Acesso em: 18/04/2019.

VANHOEF, Mathy; RONEN, Eyal. **Attacking the Dragonfly Handshake of WPA3**. Dragonblood, [S. l.], p. 1-5, 10 abr. 2019. Disponível em: <https://wpa3.mathyvanhoef.com/#usewpa3> Acesso em: 4 maio 2020.

WEARESOCIAL. Digital In 2018: **Essential Insights Into Internet, Social Media, Mobile, and Ecommerce Use Around the World. We Are Social**, [s.l.], v. 1, n. 1, p.1-153, jan. 2018. Disponível em: <https://digitalreport.wearesocial.com/report_download>. Acesso em: 01/10/2018.

WEIDMAN, Georgia. **Testes de Invasão: Uma introdução a prática ao hacking**. São Paulo: Novatec, 2016. 575 p.

WI-FI ALLIANCE. Apresenta segurança Wi-Fi CERTIFIED WPA3™. 2018. Disponível em: <<https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security>>. Acesso em: 21/04/2019.

WILHELM, Thomas. **Professional Penetration Testing: Creating and Learning in a Hacking Lab**. Tradução . [s.l.] Elsevier Science, 2018.

XAVIER, Izabella; OLIVEIRA, Pedro; FELEOL, Alex. **Segurança em Redes Wireless Domésticas: Um Estudo de Caso**. Segurança em Redes Wireless Domésticas: Um Estudo de Caso. 2017. 10 f. TCC (Graduação) - Curso de Ciência da Computação, Fundação Centro de Análise, Pesquisa e Inovação Tecnológica – Fucapi, Manaus, 2017. Disponível em: <<https://slidex.tips/download/segurana-em-redes-wireless-domesticas-um-estudo-de-caso#>>. Acesso em: 25/05/2019.

ZAMPERLINI, Paulo Roberto Tercio; SANTOS, Guilherme Rezende dos. **Protocolo de Segurança Wireless (WEP, WPA, WPA2): Um Estudo Comparativo**. 2016. 7 f. TCC (Graduação) - Curso de Sistemas de Informação, Instituto Nacional de Telecomunicações, Minas Gerais, 2016. Disponível em: <<https://www.inatel.br/biblioteca/todo-docman/pos-seminarios/seminario-de-redes-e-sistemas-de-telecomunicacoes/v-srst/9542-protocolos-de-seguranca-wireless-wep-wpa-wpa2-um-estudo-comparativo/file>>. Acesso em: 16/04/2019.

APÊNDICE A – ARTIGO

ANÁLISE DE SEGURANÇA EM REDES WIRELESS POR MEIO DO TESTE DE PENETRAÇÃO

Prof. Me. Paulo João Martins¹, Lurian Vieira Serafim¹

¹Universidade do Extremo Sul Catarinense (UNESC)

CEP:88806-000 – Criciúma – SC – Brasil

pjm@unesc.net, lurian.v.s@unesc.net

Abstract. *Wireless networks have become extremely important in the life of today's society, being used every day, both in the residential and business environment, attracted by the easy installation and use for the most diverse tasks when it comes to the Internet. Thinking about this problem in 2018, the new WPA3 protocol was announced, in order to have a more robust protocol and provide greater security. The present work aims to perform a safety test through Pentest, with the purpose of analyzing the WEP, WPA and WPA2 protocols, and a bibliographic review of the WPA3 protocol safety, where the information was obtained through scientific articles.*

Keywords: *Information Security. Wireless Networks. WPA3. WPA2. Pentest.*

Resumo. As redes Wireless se tornaram de extrema importância na vida da sociedade atual, sendo utilizada todos os dias, tanto no meio residencial quanto no empresarial, atraído pela fácil instalação e utilização para os mais diversos afazeres quando o assunto é Internet. Pensando nesse problema em 2018 foi anunciada o novo protocolo WPA3, com intuito de ter um protocolo mais robusto e fornecer maior segurança. O presente trabalho tem por objetivo realizar teste de segurança por meio de Pentest, com a finalidade de análise dos protocolos WEP, WPA e WPA2, e revisão bibliográfica da segurança do protocolo WPA3, onde as informações foram obtidas por meio de artigos científicos.

Palavras-chave: Segurança da Informação. Redes Wireless. WPA3. WPA2. Pentest.

1. INTRODUÇÃO

Com a evolução tecnológica e a convergência das redes de nova geração, o Wireless tornou-se onipresente nos ambientes corporativos. Segundo a União Internacional das Telecomunicações, órgão vinculado à Organização das Nações Unidas (ONU), em 2015, o número de internautas no mundo já era de 3,2 bilhões (G1, 2015), hoje esse número ultrapassa os 4 bilhões, segundo o serviço online Hootsuite e We Are Social, com destaque para o Brasil.

A WI-FI ALLIANCE é uma das principais empresas, que atua nesse meio, agindo sem fins lucrativos, juntamente com outras empresas, padroniza as redes Wireless, sempre com muito zelo para evitar conflitos e assim tornar o Wi-Fi uma das tecnologias mais valorizadas e grandemente utilizadas no mundo. Portanto, relacionado à grande soma de pessoas conectadas e a ampla necessidade de estar sempre à frente sobre a segurança de ponta, que o presente trabalho, estudou as tecnologias de protocolos adotados pelos roteadores Wi-Fi (WEP-WPA-WPA2-WPA3), descrevendo as melhorias obtidas com o novo protocolo WPA3 através de uma revisão bibliográfica em relação a sua antecessora WPA2.

2. JUSTIFICATIVA

Manter as conexões Wi-Fi protegidas é algo necessário para assegurar os dados pessoais dos usuários, pois o número de dispositivos Wi-Fi em uso tem crescido em todo o mundo (WI-FI ALLIANCE, 2018; tradução nossa). Todos os anos são cometidos milhões de ataques, por hackers a redes Wi-Fi. O ano de 2017 foi marcado por inúmeros ataques, estatísticas levantadas pela *Norton* (2018), 978 milhões de pessoas em 20 países vieram a ser afetadas pelo *cibercrime* em 2017; 44% dos consumidores foram impactados nos últimos 12 meses.

Como resultado das informações, os consumidores que foram vítimas de modo global perderam US\$ 172 bilhões - uma média de US\$ 142 por vítima – Com destaque novamente para o Brasil, que ficou em segundo lugar, com prejuízo de US\$ 22,5 bilhões (NORTON, 2018, tradução nossa). Com base nessas situações, no ano de 2018, iniciou-se uma melhoria na linha do WPA, em roteadores sem fio, o WPA3,

produzido pela *WI-FI ALLIANCE*. O protocolo de certificação de segurança WPA3 (2018) oferece algumas atualizações relevantes ao protocolo WPA2 criado em 2004.

A maior Mudança que o WPA3 apresentou foi a Autenticação Simultânea de Iguais do inglês *Simultaneous Authentication of Equals* (SAE) é uma nova forma de reconhecimento de um dispositivo que pretende se conectar a uma rede. Uma transformação do chamado *Dragonfly Handshake* que usa protocolo para evitar que um interceptador adivinhe uma senha, a SAE estabelece exatamente como um novo dispositivo, ou usuário, deve “saudar” um roteador de rede quando eles trocam chaves criptográficas. Segundo Koziol (2018) espera-se solucionar boa parte das vulnerabilidades existentes em um roteador Wi-F, com a nova criptografia WPA3 e assim possibilitar ao usuário se sentir mais seguro ao navegar.

3. REDES WIRELESS

Segundo Tanenbaum (2003) conceitua “rede” como um conjunto de computadores autônomos interconectados por uma única tecnologia. Proporcionado pela facilidade de conexão a Internet, as redes Wireless tem modificado de forma satisfatória o cenário de residências, escolas, escritórios, fábricas e semelhantes, se tornando cada vez mais interessante e necessário, levando em consideração que cada vez mais objetos tecnológicos em geral necessitam da conexão de rede Wireless para seu funcionamento. A rede Wireless está presente em ambientes públicos quanto em ambientes privados, empresariais, pelo fato de facilitar em grande proporção as atividades dentro da empresa.

Opera com o padrão 802.11b que foi criado entre 1999 e 2001, denominado de “O Rei Dominante”, pelo feito de se popularizar, contar com a maior base instalada e possuir grandes produtos e recursos de administração acessíveis no mercado atual, opera a frequência de 2.4 GHz possibilitando transmissões de até 11Mbit/s, suporta no máximo 32 clientes conectados. Este padrão está sendo substituído aos poucos pelo padrão g com maior velocidade (BARBOSA et al., 2017).

4. VULNERABILIDADES EM WIRELESS

Por transmitir dados através do ar por meio de sinais de rádio frequência, as redes Wireless requerem uma maior atenção por parte de todos (usuários), pois, deve-se levar em conta que essa tecnologia se propaga num meio que não oferece garantia de segurança de alcance amplo, muito maior que as redes cabeadas (BARBOSA et al., 2017). Considerando o avanço da tecnologia e da própria rede Wireless, nos quesitos desempenho e principalmente segurança, os ataques a esse modelo de rede se tornaram muito frequentes tornando-se algo infelizmente comum. Penetration Testing (Pentest) ou teste de intrusão é um processo utilizado para analisar o nível de segurança de uma determinada rede, ou melhor, avaliar as vulnerabilidades da infraestrutura de uma rede ou sistemas operacionais. O Pentest permite analisar a real estrutura do sistema, que é diagnosticada em todas as áreas inerentes à estrutura de segurança por um auditor. É de suma importância os testes aplicados, pois é através deles que é possível verificar as falhas em hardware e software utilizados, dependendo dos ataques, assim criar opções de defesas ou ajustes adequados (ROCHA et al, 2016).

4.1 ATAQUE DE DESIDENTIFICAÇÃO

O ataque de autenticação ocorre quando um cliente IEEE 802.11 seleciona um AP para usar a fim de se comunicar, ele tem o dever de primeiramente se autenticar no AP antes que a comunicação seja iniciada. Como resultado o AP ou cliente sairá do estado autenticado e recusará todos os outros pacotes até que a autenticação seja restabelecida. Quanto ao tempo que o restabelecimento necessita, depende do tempo que o cliente levará para tentar se autenticar novamente e de quaisquer timeouts ou backoffs de alto nível que possam fornecer a demanda por comunicação (BELLARDO; SAVAGE, 2003).

4.2 ATAQUE DE *HANDSHAKE*

Para um cliente se conectar a um AP, o mesmo deve primeiro ter a confiança que o cliente possui permissão para entrar na rede e dar a ele a chave que será

utilizada no protocolo de dados. Afim de realizar o ataque de dicionário off-line, o invasor irá passivamente monitorar os pacotes que vão de um cliente a um AP. Sendo que a conexão Wireless utiliza frequências e envia informações através do ar, um adversário pode escutar os pacotes destinados a um AP específico e obtê-los. A frase secreta candidata é usada para derivar o Pairwise Master Key (PMK), que é uma função de derivação de chave baseada em Password-Based Key Derivation Function 2 (PBKDF2) do Pre-Shared Key (PSK), derivada da frase secreta, o Service Set Identifier (SSID) do AP e uma função Hash Message Authentication Protocol (HMAC) (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

4.3 ATAQUE EVIL TWIN

Um ataque muito simples e conhecido é o Attack-Evil Twin Attack ou Ataque dos Gêmeos Maus que se trata de enganar o cliente para que o mesmo pense que está se conectando a um AP genuíno, quando na verdade está se conectando a um AP desonesto. O invasor encaminhará o acesso à Internet de modo que o usuário obterá o que quiser e não suspeitará de nada, mas o invasor atua como um proxy, que visualiza todos os dados em primeira mão (KOHLIOS; HAYAJNEH, 2018, tradução nossa).

5. PROTOCOLO WEP

A versão 1 foi elaborada como uma solução intermediária proposta a compensar as deficiências criptográficas do WEP sem impor a aquisição de um novo hardware e faz utilização do Temporal Key Integrity Protocol (TKIP) para protocolo. Um aperto de mão de quatro vias, demonstrado na Figura 1, é feito usando as teclas TKIP, resultando em uma chave de 512 bits que é distribuída entre o cliente e o ponto de acesso.

Uma chave temporal de 128 bits e duas chaves MIC de 64 bits são derivadas desta chave de 512 bits. Um deles é o uso do mesmo algoritmo de protocolo RC4 em vez de algo superior, como o AES, e o fato de ter duas ou mais chaves RC4 computadas sob o mesmo Initialization Vector (IV) facilita o cálculo da Temporal Key (TK) por um atacante (ZAMPERLINI; SANTOS, 2016). De acordo com pesquisas na

área, há menor rendimento médio e maior sobrecarga quando se usa WPA-TKIP quando comparado ao rendimento e sobrecarga quando se utiliza WEP (KOHLIOS; HAYAJNEH, 2018, tradução nossa). Se um invasor coletar algumas chaves RC4 calculadas sob o mesmo IV, ele será capaz de recuperar a chave TK e a chave MIC, que é usada para identificar pacotes forjados.

5.2 PROTOCOLO WPA2

O WPA2 foi desenvolvido para a obtenção de um nível de segurança ainda maior que no padrão WPA (KOHLIOS; HAYAJNEH, 2018, tradução nossa). Um nonce é um valor aleatório que é visto pelo remetente para analisar o conteúdo que o receptor tem conhecimento sobre a informação, que está sendo transmitida através dos AP's e o cliente.

A protocolo CCMP recebe a chave de protocolo PTK ou GTK (se a mensagem for unicast ou broadcast, respectivamente) e a executa por meio de um algoritmo de protocolo AES em conjunto com os cabeçalhos e sinalizadores 802.11, endereço MAC do transmissor, o número do pacote da mensagem e alguns contadores que são indispensáveis para o modo contador no AES (KOHLIOS; HAYAJNEH, 2018, tradução nossa). Isso cria 11 chaves para ser utilizada em 10 ciclos, a primeira das quais é usada para a inicialização do protocolo e a última usada para a inicialização da decodificação.

Este algoritmo é conhecido como seguro devido a sua complexidade proporcionada pelo tamanho da chave, bem como à complexidade das mudanças que, como já mencionado, criam em uma combinação de substituições em cada rodada (KOHLIOS; HAYAJNEH, 2018, tradução nossa). WPA2 também possibilita que os dados do sistema, conhecidas como quadros de gestão, sejam enviados em pacotes de texto comum do cliente para o AP. Com essa insegurança, um invasor pode alterar os pacotes para fazer parecer que os mesmos estão vindos do cliente alvo e ataques de pré-forma, como o de authentication.

5.3 PROTOCOLO WP3

Lançado em 25 de junho de 2018, o WPA3 é o mais atual sistema de segurança elaborado para reforçar a segurança em redes Wi-Fi existentes e erradicar os

problemas encontrados nas versões precedentes (KOHLIOS; HAYAJNEH, 2018, tradução nossa). Com base na grande utilização do WPA2 durante mais de uma década, o WPA3 inclui novos recursos para facilitar a segurança Wi-Fi, proporcionar autenticação mais robusta e produzir maior força criptográfica para mercados de dados demasiado confidenciais. Todas as redes WPA3 usam os recursos de segurança mais atuais não permitindo protocolos legados desatualizados e exigem o uso de Protected Management Frameworks (PMF) para manter a resiliência das redes de missão crítica (WI-FI ALLIANCE, 2018, tradução nossa).

Com o Easy Connect, que nada mais é que uma nova funcionalidade opcional, mas que veio para facilitar a vida dos usuários, em vez de incluir senhas toda vez que precisar adicionar algo a rede, os dispositivos terão códigos QR code exclusivos: o código para cada dispositivo funcionará como uma espécie de chave pública. Isso também evita a chamada injeção de pacote não sofisticada, na qual um invasor tenta alterar as operações da rede, construindo e transmitindo pacotes de dados que parecem fazer parte das operações comuns da rede (WI-FI ALLIANCE, 2018, tradução nossa).

6. RESULTADOS

Com os testes de *Pentest* realizados com os protocolos WEP, WPA, WPA2 observou-se os seguintes resultados. Foi concluída que o protocolo WEP em suas versões 64 e 128 bits, é o mais fraco protocolo, pois mesmo na versão 128 bits sendo possível fazer o uso de uma senha mais complexa do que na versão 64bits, o protocolo é quebrado e a senha descoberta sem maiores dificuldades. Já com os protocolos WPA e WPA2, mesmo sendo mais robustas e necessitarem da descoberta de mais dados juntamente com um ataque mais elaborado, também se mostraram vulneráveis aos ataques ministrados, mesmo quando utilizado uma senha maior com caracteres maiúsculos, minúsculos, especiais e números juntos as mesmas eram quebradas e suas senhas descobertas.

Com relação ao protocolo WPA3, baseando-se nos artigos científicos e todo o estudo feito sobre os protocolos, trouxe melhorias com relação a sua antecessora o protocolo WPA2, porém também herdou algumas de suas vulnerabilidades, que

mesmo necessitando de um ataque mais elaborado ainda se faz possível aproveitar-se dessas vulnerabilidades para realizar a quebra do protocolo e descobrir a senha da mesma. Levando em consideração todas as informações presentes neste trabalho é possível observar, que uma configuração correta do AP se faz necessária, com intuito de auxiliar os protocolos no quesito segurança como, por exemplo, a função WPS, que como mencionado com os resultados obtidos se fez resistente aos testes de Pentest ministrados, porem como a tecnologia está em constante desenvolvimento e com ela os tipos de ataques evoluem e também novos são criados, e levando em consideração que mesma não se faz necessária para a utilização de uma rede *Wireless*, poderia ser desativada sem problemas.

A utilização dos mais novos protocolos sendo ela o WPA2 ou WPA3, com uma senha robusta e bem elaborada, pois mesmo que não garanta segurança total cria um obstáculo que dificulta ao máximo a invasão do AP. E por último realizar a troca periódica da senha pode ser de grande auxilio e garantir a segurança.

7. COMCLUSÃO

O presente trabalho por meio dos testes de *Pentest* demonstrou a falta de segurança nos protocolos WEP, WPA, e WPA2, já com relação ao novo protocolo WPA3, mesmo não conseguindo obtê-lo para realização dos testes de *Pentest* como foi realizado com as demais protocolos tendo em vista os motivos já mencionados, os resultados e conclusões foram obtidos com base nas pesquisas bibliográficas.

Com o avanço da tecnologia infelizmente os métodos de invasão os protocolos se tornam cada vez mais robustos, tendo em vista isso se fez necessário à criação do protocolo WPA3. Sendo o mesmo um protocolo superior, infelizmente como demostram os resultados e discussões, o mesmo não supriu as necessidades de segurança necessárias nos dias atuais, trazendo consigo vulnerabilidades importantes que inclusive foram herdadas de seu antecessor o protocolo WPA2, como por exemplo a vulnerabilidade de retrocompatibilidade, que explora a compatibilidade do protocolo WPA3 com seu antecessor o WPA2, tendo em vista que no primeiro momento os dispositivos não terão total compatibilidade com o novo protocolo WPA3, assim que o mesmo se fizer amplamente presente nos AP's.

Sendo assim é cada vez mais importante que seja observado a configuração correta dos AP's, como por exemplo utilizar sempre o protocolo de segurança mais atual, sendo eles o WPA2 ou WPA3, realizar a utilização de um senha robusta composta por números, letras e caracteres especiais e sempre que possível substituí-la por uma por uma nova como forma de elevar a segurança e assim auxiliar o protocolo escolhido, pois se sabe que em alguns casos a má configuração do mesmo acaba acarretando mais problemas à segurança que as próprias falhas dos protocolos e criptografias.

Juntamente com as boas práticas de utilização, que devem ser amplamente empregadas por todos os usuários para garantir, que por meio da má utilização o AP utilizado não exponha os dados e nem que o mesmo sofra, com ataque relacionado a vírus e malwares. Com relação às senhas como já mencionado, devem se dar a atenção necessária, pois elas podem vir a se tornar uma forma muito eficaz de evitar ataques as redes *Wireless* pois mesmo com o avanço da tecnologia e o surgimento do novo protocolo WPA3, ainda há muita dificuldade em garantir a segurança de informações que trafegam por meio dos AP's, e ao empregar senhas robustas as mesma se torna um ótimo obstáculo contra os ataques.

Com o protocolo WPA3 espera-se que o mesmo receba atualizações para que se torne ainda mais robusto, pois assim de fato possa vir a substituir a sua antecessora com o devido propósito a que lhe foi atribuído em sua criação. Recomenda-se para trabalhos futuros, sugerindo para que tendo em posse de um AP com o protocolo WPA3, reavaliar a protocolo, a fim de verificar se houve atualizações que gerem melhoria do mesmo, e assim sanar os problemas apontados nesse trabalho.

8. REFERÊNCIAS

BARBOSA, Gracieiny A. et al. **Estudo de Caso: Vulnerabilidades em Rede Wireless**. Revista Gestão em Foco, São Paulo, v. 9, n. 9, p.1-20, mar. 2017. Disponível em: < http://www.unifia.edu.br/revista_eletronica/revistas/gestao_foco/artigos/ano2017/057_estudo10.pdf>. Acesso em: 20/05/2019.

KOHLIOS, Christopher; HAYAJNEH, Thaier. **A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3**. *Electronics*, [s.l.], v. 7, n. 11, p.284-

312, 30 out. 2018. MDPI AG. <http://dx.doi.org/10.3390/electronics7110284>. Acesso em: 15/05/2019.

NORTON. **Norton Cyber Security Insights Report Global Results**. Symantec, U. S, 2018. Disponível em: <<https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf>>. Acesso em: 21/04/2019.

WI-FI ALLIANCE. Apresenta segurança Wi-Fi CERTIFIED WPA3™. 2018. Disponível em: <<https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security>>. Acesso em: 21/04/2019.